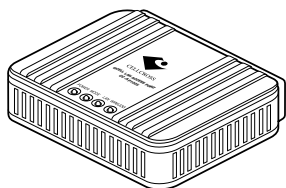
取扱説明書

# @CELL

@CELL LAN ACCESS POINT

# CC-AP1005

[IEEE802.11n]規格準拠
[IEEE802.11a(W52)/b/g]規格準拠
[IEEE802.3af]規格PoE準拠



5.2GHz帯無線LANの使用は、電波法により、屋内に限定されます。

CELLCROSS Co., Ltd.

# はじめに

このたびは、本製品をお買い上げいただきまして、まことにありがとうございます。

本製品は、[IEEE802.11a(W52)]規格※1、[IEEE802.11b/g]規格※2、[IEEE802.11n]規格※3に準拠する@CELL LANアクセスポイントです。

ご使用の前に、この取扱説明書をよくお読みいただき、本製品の性能を十分発揮していただくとともに、末長くご愛用くださいますようお願い申し上げます。

※1 [IEEE802.11a]規格の無線LANについて
[IEEE802.11a(W52/W53)]：5.2/5.3GHzの無線LAN規格
[IEEE802.11a(W56)]　　　：5.6GHzの無線LAN規格
本製品は、[IEEE802.11a(J52/W53/W56)]規格とは通信できません。
※2 [IEEE802.11g]規格の無線LANについて
[IEEE802.11b]規格の無線LANと互換性があります。
[IEEE802.11]規格(14CH)とは通信できません。
※3 [IEEE802.11n]規格の無線LANについて
[IEEE802.11a/b/g]規格と互換性があります。

**5.2GHz帯無線LANの使用は、電波法により、屋内に限定されます。**

# 登録商標等について

セルクロス、◆、@CELLは、株式会社セルクロスの登録商標です。
本製品は、株式会社セルクロスの保有する特許および技術である@CELLに基づいています。
ＬＡＮシート、LANSheetは、株式会社イトーキの登録商標です。
アイコム株式会社、アイコム、Icom Inc.、アイコムロゴは、アイコム株式会社の登録商標です。
Microsoft、Windows、Windows Vistaは、米国Microsoft Corporationの米国およびその他の国における登録商標です。
Adobe、Adobe Readerは、Adobe Systems Incorporated(アドビシステムズ社)の登録商標です。
Atherosは、Atheros Communications, Inc.の登録商標または商標です。
Wi-Fi、WPAは、Wi-Fi Allianceの商標または登録商標です。
その他、本書に記載されている会社名、製品名は、各社の商標および登録商標です。

# 無線LAN規格について

**本製品が準拠する無線LAN規格と最大通信速度の関係は、以下のとおりです。**

| 本製品が準拠する無線LAN規格 | 周波数帯 | 帯域幅モード | 最大通信速度(理論値)★ |
|---|---|---|---|
| [IEEE802.11n (W52)] | 5.2GHz | 20MHz | 130Mbps |
| | | 40MHz | 300Mbps |
| [IEEE802.11n] | 2.4GHz | 20MHz | 130Mbps |
| | | 40MHz | 300Mbps |
| [IEEE802.11a (W52)] | 5.2GHz | 20MHz | 54Mbps |
| [IEEE802.11g] | 2.4GHz | 20MHz | 54Mbps |
| [IEEE802.11b] | 2.4GHz | 20MHz | 11Mbps |

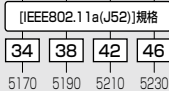
★ 最大通信速度は、実際のデータ転送速度(実測値)を示すものではありません。
※ 本製品の出荷時や設定を初期化したときは、[IEEE802.11n/a]規格で通信します。
※ [IEEE802.11n]規格は、「ath0〜ath2」の仮想APを使用し、暗号化方式を「なし」または「AES」に設定している場合に有効です。
※「ath3」の仮想APをお使いの場合は、[IEEE802.11a/b/g]規格の通信になります。
※ [IEEE802.11n/b/g]規格と[IEEE802.11n/a(W52)]規格の同時通信には対応していません。
※ [IEEE802.11g]規格は、[IEEE802.11b]規格と互換性があります。
※ [IEEE802.11a(J52/W53/W56)]規格とは通信できません。
※ [IEEE802.11](14CH)とは通信できません。

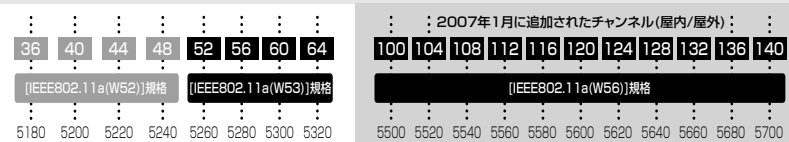
## [IEEE802.11a(W52)]規格の無線通信チャンネルについて

右に記載する記号がある製品は、[IEEE802.11a(W52)]規格で採用された無線通信チャンネルに対応した製品を意味します。
無線LAN端末についても、右に記載する記号がある製品でご使用いただくことをおすすめします。

[IEEE802.11a]規格の周波数(MHz)

**2005年5月以前の無線LAN規格**

[IEEE802.11a(J52)]規格
34 38 42 46
5170 5190 5210 5230

[IEEE802.11a(J52)]規格の無線LANが本製品の近くで稼働している環境で、本製品の[IEEE802.11n/a(W52)]規格をご使用になると電波干渉の原因になりますので、ご注意ください。

**2005年5月以降の無線LAN規格**

[IEEE802.11a(W52/W53)]規格の範囲　[IEEE802.11a(W56)]規格の範囲

# はじめに

## 本製品の概要について

◎本製品に接続したカプラを通信シート(ＬＡＮシート)に置くことにより、本製品と無線LAN端末が通信できます。

※別売品のカプラと通信シート(ＬＡＮシート)については、お買い上げの販売店にお問い合わせください。

◎[IEEE802.11a(W52)]規格、[IEEE802.11b/g]規格に加え、[IEEE802.11n]規格に準拠しています。

※[IEEE802.11n]規格は、「ath0〜ath2」の仮想APを使用し、暗号化方式を「なし」または「AES」を設定している場合に有効です。

※[IEEE802.11a(J52/W53/W56)]規格の機器とは通信できません。

◎[IEEE802.11n]規格は、2倍の周波数帯域幅と複数のカプラを使用してデータを同時に送受信することで、最大300Mbps(理論値)の速度で通信できます。
また、[IEEE802.11a(W52)/b/g]規格とも互換性がありますので、既存の無線ネットワークと通信できます。

◎異なる無線LAN規格の機器を同時に使用する環境において、[IEEE802.11n/a(W52)/b/g]規格の速度低下を緩和するプロテクション機能を搭載しています。

◎[IEEE802.1Q]のVLAN規格に準拠した仮想AP機能を搭載していますので、本製品1台で最大4グループの無線ネットワークを構築できます。

◎ネットワーク認証は、「共有キー」、「オープンシステム」、「MAC認証」、「IEEE802.1X」、「WPA」、「WPA2」、「WPA-PSK」、「WPA2-PSK」に対応しています。
「MAC認証」、「IEEE802.1X」、「WPA」、「WPA2」を設定すると、認証にRADIUSサーバーを使用できます。

◎[IEEE802.3af]規格に準拠したPoE受電機能に対応していますので、別売品の「イーサネット電源供給ユニット(SA-4)」(アイコム社製)、または市販の[IEEE802.3af]規格対応HUBから電源を供給できます。

◎「Wi-Fiアライアンス」が提唱するWPS(Wi-Fi Protected Setup)機能の搭載により、SSIDと暗号化(WPA-PSK/WPA2-PSK)を本製品(仮想AP:ath0〜ath3)、およびWPS機能対応の無線LAN端末に自動設定できます。

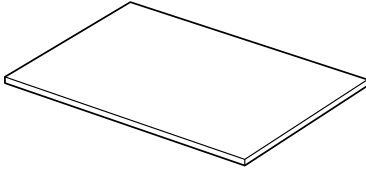
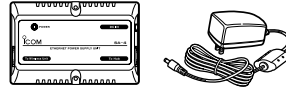
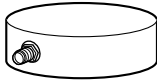
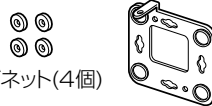
※2011年7月現在、本製品はWi-Fiアライアンスの認定を取得していません。

◎有線LANは、10BASE-T/100BASE-TX/1000BASE-Tの自動切り替えに対応し、ポートの極性についても、MDI(ストレート)/MDI-X(クロス)を自動判別します。

◎ネットワーク管理機能として、SNMPをサポートしています。

◎本製品は、免許不要･資格不要です。

## 別売品について

(2011年7月現在)



※本製品をお使いになるには、別売品のカプラと通信シート(ＬＡＮシート)が必要です。
　詳しくは、お買い上げの販売店にお問い合わせください。

【別売品についてのご注意】
本製品の性能を十分に発揮できるように設計されていますので、必ず弊社指定の別売品をお使いください。
弊社指定以外の別売品とのご使用が原因で生じるネットワーク機器の破損、故障あるいは動作や性能については、保証対象外とさせていただきますので、あらかじめご了承ください。

# はじめに

## 出荷時のおもな設定値について

| | | | | |
|---|---|---|---|---|
| ネットワーク設定 | LAN側IP | IPアドレス設定 | IPアドレス: | 192.168.0.1 |
| | | | サブネットマスク: | 255.255.255.0 |
| | DHCPサーバー | DHCPサーバー設定 | DHCPサーバー機能を使用: | しない |
| 無線設定 | 無線LAN | 無線LAN設定 | 無線UNITを使用: | する |
| | | | チャンネル: | 036CH(5180MHz) |
| | 仮想AP(ath0) | 仮想AP設定 | SSID: | CELLCROSS-0 |
| | | 暗号化設定 | 暗号化方式: | なし |
| | WPS | WPS設定 | 使用するインターフェース: | なし |
| システム設定 | 管理者 | 管理者パスワードの変更 | 管理者ID: | admin(変更不可) |
| | | | 現在のパスワード: | cellcross(半角小文字) |

※上記以外の設定値については、本書182ページ～183ページをご覧ください。
「ath0」は、出荷時に設定されている仮想AP(アクセスポイント)の名称です。

**【不正アクセス防止のアドバイス】**

本製品に設定するすべてのパスワードは、容易に推測されないものにしてください。
数字だけでなくアルファベット(大文字/小文字)や記号などを組み合わせた複雑なものにし、さらに定期的にパスワードを変更すると有効です。

## 本書の表記について

**本書は、次の表記規則にしたがって記述しています。**

「　」表記：オペレーティングシステム(OS)の各ウィンドウ(画面)、ユーティリティー、設定画面の各メニューとそのメニューに属する設定画面の名称を(「」)で囲んで表記します。

[　]表記：タブ名、アイコン名、テキストボックス名、チェックボックス名、各設定画面の設定項目名を([ ])で囲んで表記します。

〈　〉表記：ダイアログボックスのコマンドボタンなどの名称を(〈〉)で囲んで表記します。

※ Microsoft® Windows® 7 Ultimate、Microsoft® Windows® 7 ProfessionalおよびMicrosoft® Windows® 7 Home Premiumは、Windows 7と表記します。
Microsoft® Windows Vista® Ultimate、Microsoft® Windows Vista® Business、Microsoft® Windows Vista®Home PremiumおよびMicrosoft® Windows Vista® Home Basicは、Windows Vistaと表記します。
Microsoft® Windows® XP Professional、Microsoft® Windows® XP Home Editionは、Windows XPと表記します。

※本書は、Ver. 1.02のファームウェアを使用して説明しています。
※ 本書では、紙面上の都合により、設定画面の一部を省略して掲載しています。
※ 本書中の画面は、OSのバージョンや設定によって、お使いになるパソコンと多少異なる場合があります。

# はじめに

## ご使用までの流れ

**本製品を設定されるときは、次の手順にしたがってお読みください。**
順番に基本的な設定ができる構成になっています。
※右端に記載する数字は、本書の参照ページです。

# もくじ

# もくじ

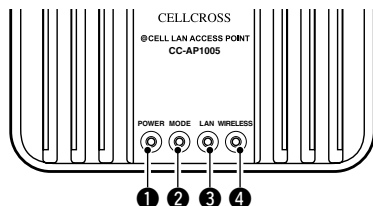
# ご使用になる前に

# 第 1 章

**この章では、<br>本製品のおもな機能などを説明しています。**

# 1. 各部の名称と機能

## 上面部

各ランプのおもな動作と状態について説明します。

❶ [POWER]ランプ …………電源と初期化操作(☞P172)の状態を表示します。

点灯(緑):本製品の電源が入っているとき

点滅　　:起動中、または設定初期化のために〈MODE〉ボタンを操作したとき(緑、橙の交互点滅)

❷ [MODE]ランプ ……………WPS機能(☞P25、P40、P143)による暗号化自動設定の状態を表示します。

点灯(緑):設定を完了したとき

消灯　　:設定完了後、5分経過したとき

　　　　:設定失敗後、20秒経過したとき

点滅　　:設定中(緑)、または設定失敗(赤)のとき

※設定中は、ゆっくり点滅(緑色)し、約2分経過すると、設定失敗となり赤色で点滅します。

❸ [LAN]ランプ ………………有線LANの状態を表示します。

点灯(緑):10BASE-T/100BASE-TXで接続したとき

点灯(橙):1000BASE-Tで接続したとき

点滅(緑):10BASE-T/100BASE-TXでデータを送受信しているとき

点滅(橙):1000BASE-Tでデータを送受信しているとき

❹ [WIRELESS]ランプ ………無線LANの状態を表示します。

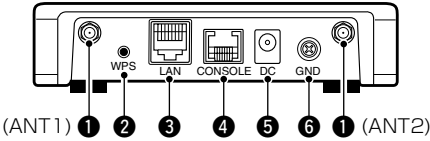
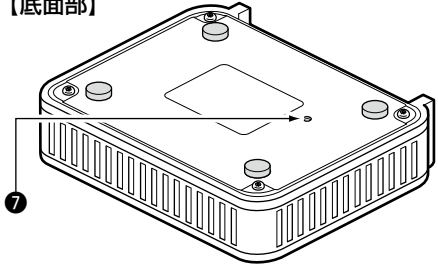
点灯(緑):本製品と2.4GHz帯で無線通信を確立したとき

点灯(橙):本製品と5GHz帯で無線通信を確立したとき

消灯　　:本製品と無線通信が確立していない、または無線通信しない状態がつづいたとき
なお、消灯までの時間は、通信状態によって異なります。

## 後面部/底面部

各ランプのおもな動作と状態について説明します。

【後面部】　　　　　【底面部】

**❶アンテナコネクター** ………別売品のカプラを接続します。(☞P17)

※カプラに付属のアッテネーターをアンテナコネクターに取り付けてから、カプラを取り付けてください。

**❷〈WPS〉ボタン** ………………WPS機能(☞P25、P40、P143)を使用して、暗号化自動設定を開始するとき使用します。

※出荷時、または全設定を初期化したときは、WPS機能の操作が無効に設定されています。

※指で押せないときは、ペン先などを利用して押してください。

**❸[LAN]ポート** ………………LANケーブル(市販品)を使用して、HUBなどのネットワーク機器を接続します。

※[1000BASE-T]規格でご使用になる場合、カテゴリー5e以上のLANケーブルをご使用ください。

**❹[CONSOLE]ポート (RJ-11型×1)** ………RS-232Cシリアルインターフェース搭載の制御機器と接続して、本製品を設定するとき使用します。

※接続には、アイコム社製別売品ケーブル(OPC-1402)が必要です。

**❺DCジャック** …………………付属のACアダプターを接続します。

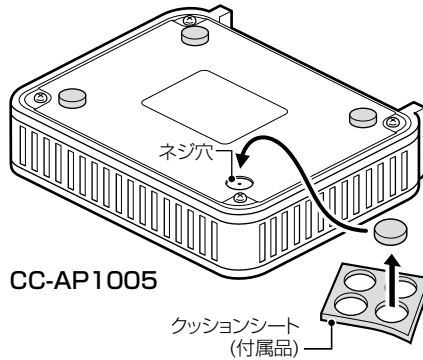
※本製品の[LAN]ポートに、イーサネット電源供給ユニット(別売品：SA-4)、または[IEEE802.3af]対応のHUBを接続するときは、付属のACアダプターを接続する必要はありません。

**❻アース端子** …………………アース線(市販品)を接続します。

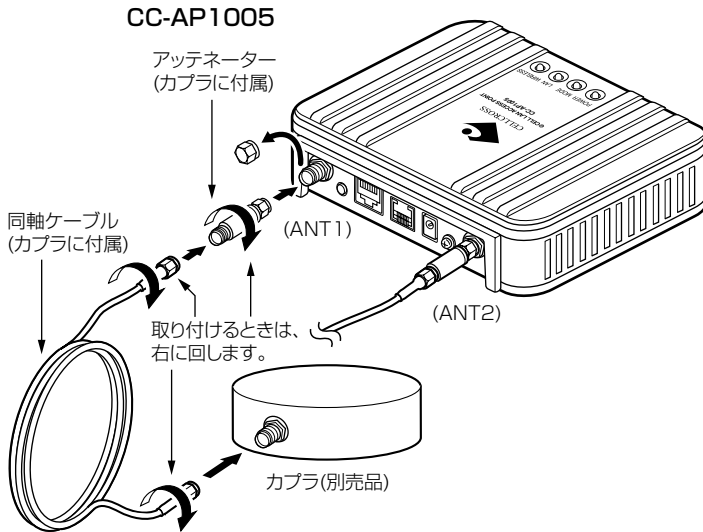
**❼〈MODE〉ボタン** ……………設定を初期化するとき使用します。(☞P172)

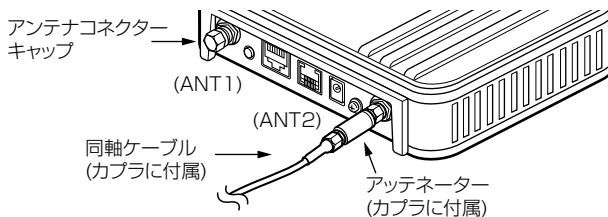
※ペン先などを利用して押してください。

## 2. クッションの取り付けの取り付けかた

クッションは、シートからはずして、下記のように本製品の底面部に貼り付けます。
※ 丸く型抜きされたクッションが4個、粘着面を保護するシートの上に付いています。

**⚠注意**
クッションを貼り付ける位置のネジ穴は、MB-102(別売品)の取り付けに使用しますので、MB-102の取り付け以外には使用しないでください。
内部の部品を破損する原因になります。

## 3. カプラ(別売品)の取り付けかた

本製品のアンテナコネクターとカプラ(別売品)を、カプラに付属しているアッテネーターと同軸ケーブルを使用して接続します。
このとき、コネクター部がゆるまないよう、確実に締まっていることを確認してください。
※通信シート上のカプラ(別売品)、または無線LAN端末を少し移動すると、通信速度が改善することがあります。

**カプラを1個だけ接続するときは**

◎本製品の設定画面にアクセスして、「無線設定」メニューにある[無線LAN設定]項目にある[ストリーム数(Tx×Rx):]欄の設定を「1×1」に変更してください。(☞P96)
◎カプラに付属しているアッテネーターと同軸ケーブルを、後面パネルから見たとき右側のコネクター(ANT2)に接続してください。

## 3. カプラ(別売品)の取り付けかた

接続するカプラ数や本製品の設定により、お使いになる無線LAN規格の最大通信速度が異なります。

### [IEEE802.11n(W52)]規格の場合

| 周波数帯 | 帯域幅モード | 利用できるチャンネル | チャンネル数★ | 最大通信速度(理論値) | カプラ数 | ストーム数設定 | 最低レート制限 |
|---|---|---|---|---|---|---|---|
| 5.2GHz | 20MHz | 36/40/44/48 | 4 | 65 | 1 | 1×1 | 36Mbps |
| | 20MHz | 36/40/44/48 | 4 | 130 | 2 | 2×2 | 36Mbps |
| | 40MHz | 36/44 | 2 | 150 | 1 | 1×1 | 36Mbps |
| | 40MHz | 36/44 | 2 | 300 | 2 | 2×2 | 36Mbps |

### [IEEE802.11n]規格の場合

| 周波数帯 | 帯域幅モード | 利用できるチャンネル | チャンネル数★ | 最大通信速度(理論値) | カプラ数 | ストーム数設定 | 最低レート制限 |
|---|---|---|---|---|---|---|---|
| 2.4GHz | 20MHz | 1～13 | 3 | 65 | 1 | 1×1 | 36Mbps |
| | 20MHz | 1～13 | 3 | 130 | 2 | 2×2 | 36Mbps |
| | 40MHz | 1～9 | 1 | 150 | 1 | 1×1 | 36Mbps |
| | 40MHz | 1～9 | 1 | 300 | 2 | 2×2 | 36Mbps |

### [IEEE802.11a(W52)]規格の場合

| 周波数帯 | 帯域幅モード | 利用できるチャンネル | チャンネル数★ | 最大通信速度(理論値) | カプラ数 | ストーム数設定 | 最低レート制限 |
|---|---|---|---|---|---|---|---|
| 5.2GHz | 20MHz | 36/40/44/48 | 4 | 54 | 1 | 1×1 | 36Mbps |

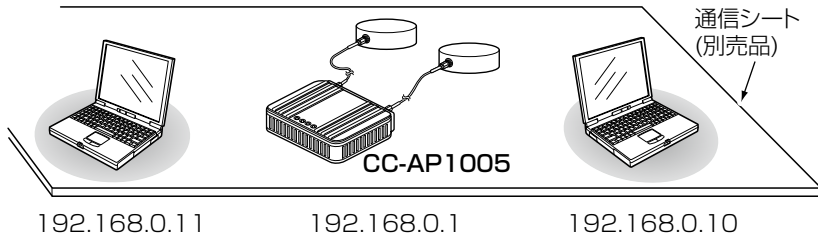
### [IEEE802.11g]規格の場合

| 周波数帯 | 帯域幅モード | 利用できるチャンネル | チャンネル数★ | 最大通信速度(理論値) | カプラ数 | ストーム数設定 | 最低レート制限 |
|---|---|---|---|---|---|---|---|
| 2.4GHz | 20MHz | 1～13 | 3 | 54 | 1 | 1×1 | 36Mbps |

★チャンネルを設定されるときは、電波干渉を防止するため、別の無線ネットワークグループと4チャンネル以上空けてください。

# 4. 本製品のおもな機能

## アクセスポイント機能について

本製品は、[IEEE802.11n/a(W52)/b/g]規格の無線アクセスポイントとして機能します。
※ 出荷時、本製品は、[IEEE802.11n/a]規格の無線LAN端末と通信します。
※ [IEEE802.11n/b/g]規格と[IEEE802.11n/a (W52)]規格の同時通信には、対応していません。
※ [IEEE802.11]規格(14CH)の無線LAN端末とは通信できません。

【例】 [IEEE802.11a]規格の「036CH」で通信する無線LAN端末



### 同時に使用できる無線LAN端末の台数について

本製品に多くの無線LAN端末が同時にアクセスすると、通信速度が著しく低下することがあります。
同時に使用できる無線LAN端末の台数は、接続端末制限機能(☞P22、P103)で仮想APごとに制限(最大63台)されます。
異なる無線LAN規格の混在による電波干渉で、[IEEE802.11n]規格の通信速度が著しく低下する場合は、[プロテクション機能](☞P99)と併せてご使用ください。

## 4. 本製品のおもな機能

### 無線LANセキュリティー

本製品は、無線LAN通信に必要な次のセキュリティーを搭載しています。
詳細については、本書5章をご覧ください。

※対応する無線LAN製品について詳しくは、本書7章をご覧ください。

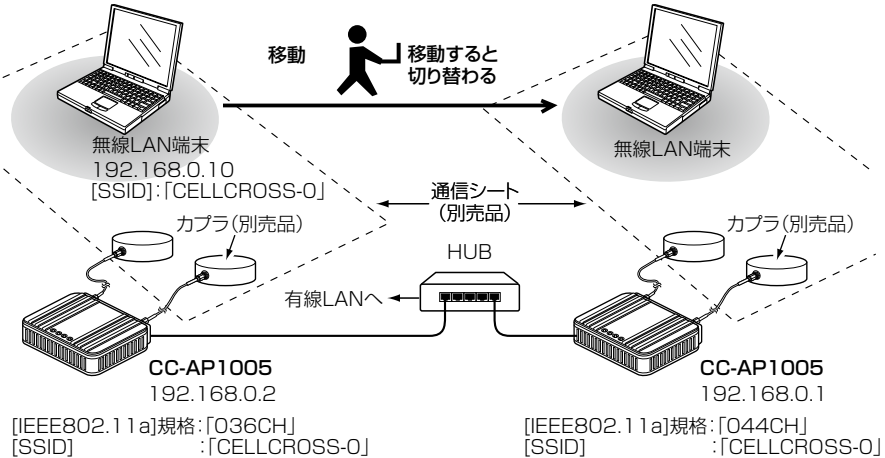
- **MACアドレスフィルタリング**
  あらかじめ本製品の各仮想AP(ath0～ath3)に登録されたMACアドレスを持つ無線LAN端末だけにアクセスを許可、または拒否するとき使用します。
- **WEP RC4※1**
  無線通信で一般によく使用されるセキュリティーです。
  無線ネットワーク間で送受信するデータを、設定された文字列を元に暗号化して安全性を確保します。
- **TKIP/AES※2**
  Windows標準のワイヤレスネットワーク接続で使用できる暗号化方式です。
- **MAC認証**
  MAC認証は、無線LAN端末のMACアドレスをRADIUSサーバーで認証します。
- **WPA/WPA2**
  RADIUSサーバーで「IEEE802.1X」認証をします。
- **WPA-PSK/WPA2-PSK**
  RADIUSサーバーを使用しない簡易的な認証方式で、共有鍵(キー)を使用します。
- **IEEE802.1X※3**
  RADIUSサーバーを使用して、無線LAN端末からのアクセスにユーザー認証を設ける機能です。

※1 通信相手と暗号化方式や鍵(キー)の設定が異なるときは、通信できません。
「WEP RC4 152(128)」方式は、Windows標準のワイヤレスネットワーク接続を使用して本製品に接続できません。
※2 「TKIP」は、「WEP RC4」より強力な暗号化方式です。
「AES」は、「TKIP」より強力な暗号化方式です。
[IEEE802.11n]規格は、「ath0～ath2」の仮想APを使用し、暗号化方式を「なし」または「AES」を設定している場合に有効です。
※3 WEP RC4以外の暗号化方式では使用できません。

**【不正アクセス防止のアドバイス】**

本製品に設定する暗号鍵(WEPキー)/共有鍵(Pre-Shared Key)は、容易に推測されないものにしてください。
数字とアルファベット(大文字/小文字)を組み合わせた複雑なものにし、さらに定期的に暗号鍵/共有鍵を変更すると有効です。

## ローミング機能

無線LAN端末を移動させても、自動的に電波状況のよい別の無線アクセスポイント(本製品)に切り替えることによって、無線LANが利用できる機能です。

### ローミング機能を使用するには

◎ 有線LANに接続する本製品と無線LAN端末は、無線ネットワーク名(SSID)や暗号化をすべて同じ設定にしてください。

◎ DHCPサーバー機能が「する」に設定された本製品などが同一ネットワーク内に複数存在すると、IPアドレスが重複して不測の事態になりますので、接続にはご注意ください。
※出荷時、本製品のDHCPサーバー機能は、「しない」に設定されています。

◎ 本製品に多くの無線LAN端末、または異なる無線LAN規格の端末が混在する環境でご使用になる場合は、電波干渉しないチャンネルを設定してください。
[IEEE802.11g]規格では、相手側と4チャンネル以上空けて設定してください。
各無線LAN規格での電波干渉を回避するための説明については、[チャンネル:]欄(☞P91～P95)、および[プロテクション機能:]欄(☞P99)をご覧ください。

## 4. 本製品のおもな機能

### 無線ネットワーク名(SSID)について

本製品と無線LAN端末には、接続先を識別するための無線ネットワーク名として、SSID(またはESS ID)が設定されています。(☞P38、P101)
※異なる[SSID]を設定している無線LAN端末とは接続できません。
※無線LAN端末側で「ANY」に設定されていると、本製品の[SSID]の設定に関係なくこの無線LAN端末から接続できます。
「ANY」に設定されている無線LAN端末からの接続を拒否する場合、[ANY接続拒否]を「する」に変更してください。(☞P102)
[ANY接続拒否]とWPS機能(☞P25、P40)との併用は、できません。
※仮想AP機能(☞P24、P47)を使用する場合、同じ[SSID]を各仮想APに設定できません。

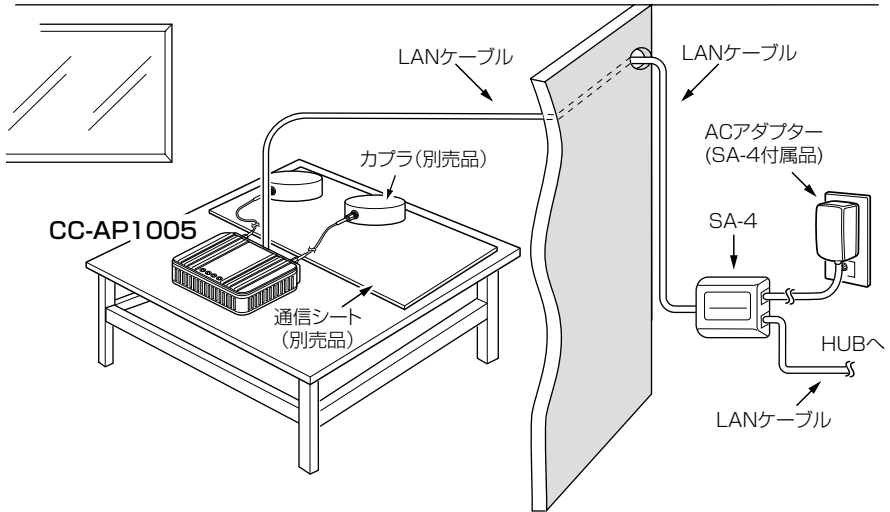
### 接続端末制限機能

本製品の仮想APごとに同時接続できる無線LAN端末の台数を制限して、接続が集中するときに起こる通信速度の低下を防止する機能です。(☞P103)
※出荷時、仮想APごとに最大63台に設定されています。

### [IEEE802.11n]規格

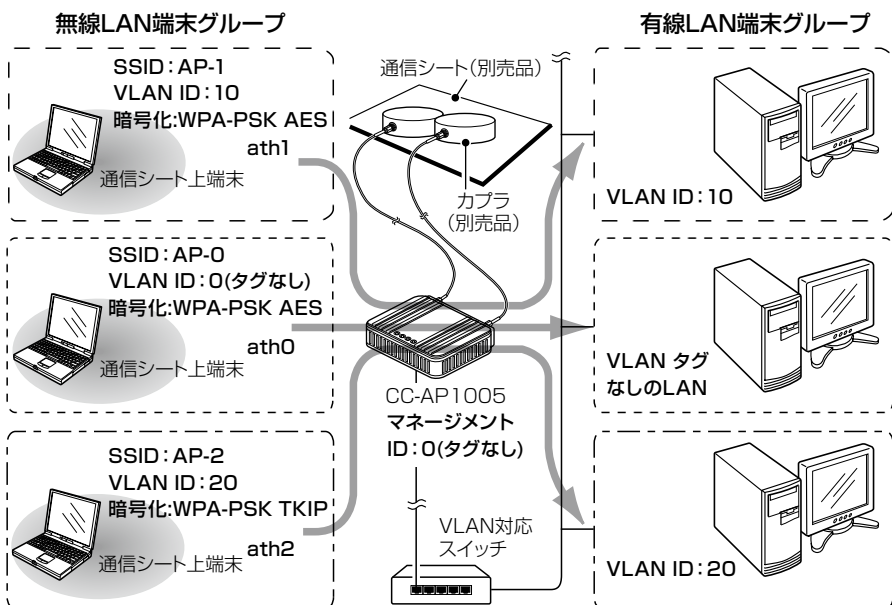
２倍の周波数帯域幅と複数のアンテナを使用してデータを同時に送受信することで、最大300Mbps★(理論値)の速度で通信できます。
★[IEEE802.11n]規格は、「ath0～ath2」の仮想APを使用し、暗号化方式を「なし」または「AES」に設定している場合に有効です。
さらに、最大300Mbps(理論値)で使用するには、5.2/2.4GHz帯のチャンネルで、「40MHz帯域幅モード」(☞P91)を設定してください。
※「ath3」の仮想APをお使いの場合は、[IEEE802.11a/b/g]規格の通信になります。
※[IEEE802.11a(W52)/b/g]規格と互換性があります。
※最大通信速度については、3ページ、18ページをご覧ください。

## PoE機能について

本製品の設置場所付近にコンセントや[IEEE802.3af]規格対応のHUBがない場合に備えて、別売品のイーサネット電源供給ユニット(アイコム社製SA-4)をご用意しています。
SA-4をお使いいただくことで、本製品の[LAN]ポートから電源を受電できます。
※接続について詳しくは、本書186ページをご覧ください。

## 4. 本製品のおもな機能

### 仮想AP機能

本製品1台で、条件(SSID/暗号化認証/暗号化方式/VLAN ID)の異なる無線LAN端末グループを複数構成できます。

※下記の図は、「ath0」〜「ath2」を異なる無線LAN端末グループの仮想APとして使用する例です。
設定例については、本書47ページをご覧ください。

※上記の図では、[SSID]を「AP-1」と「AP-2」に設定する無線LAN端末グループが、本製品の仮想APグループとして稼働している例です。
※無線LAN端末グループのパソコン(3台)は、通信シートの上に置かれているものとします。

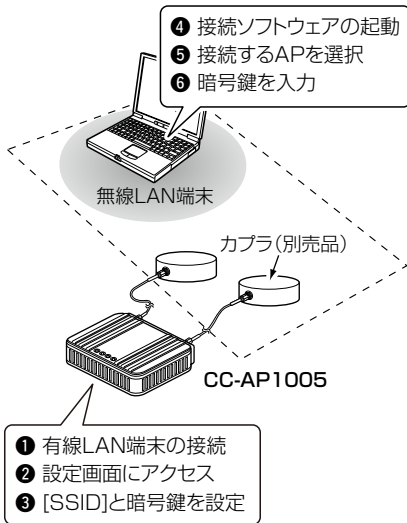
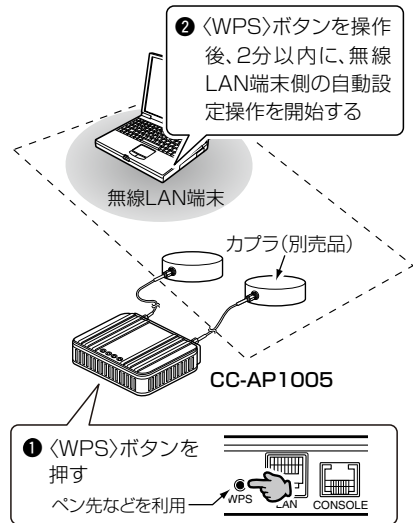
#### 仮想AP機能を使用するには

◎ 各仮想AP(ath0〜ath3)の無線LAN端末グループには、VLAN ID(0〜4094)を設定できます。
◎ [SSID]がほかの仮想APと重複する場合は、登録できません。
◎ 最大4グループ(ath0〜ath3)の仮想APを使用できます。
◎ Windows標準のワイヤレスネットワーク接続を使用して、「WEP RC4」で暗号化された本製品と通信する場合、無線LAN端末側のキーインデックスを「1」に設定してください。
◎ 出荷時、本製品の[マネージメントID:]が「0」に設定されていますので、VLAN IDが設定されたネットワークからは、本製品の設定画面にアクセスできません。

## WPS機能

「Wi-Fiアライアンス」が提唱する機能で、SSIDと暗号化(WPA-PSK/WPA2-PSK)を本製品とWPS機能対応無線LAN端末に自動設定できます。

※自動設定の方法は、本製品の後面パネルにある〈WPS〉ボタンを使用する「プッシュボタン(Push Button Configuration)方式」と自動設定する相手のPINコードが必要な「PIN(Personal Identification Number)方式」を選択できます。(☞P40、P140〜P145)

**【WPS機能を使用しない場合】**

**【WPS機能を使用する場合】**

### WPS機能を使用するには

◎ WPS機能対応の無線LAN端末を準備してください。
※無線LAN端末側の自動設定については、お使いになる端末の取扱説明書をご覧ください。

◎ 本製品のWPS機能で自動設定する仮想APのインターフェース名称(ath0〜ath3)を「WPS」画面にある[使用するインターフェース]欄から選択し、そのインターフェース名称に対するWPS機能を有効に(☞P40)してください。
[使用するインターフェース]欄で仮想APのインターフェース名称が「なし」(出荷時の設定)に設定されている場合は、本製品の後面パネルにある〈WPS〉ボタンを使用できません。
また、本製品の設定画面にも〈開始〉ボタンが表示されません。

# 接続ガイド　第2章

**この章では、**
**本製品をご使用いただくために必要な基本設定の手順を説明しています。**



## DHCPサーバー機能について

出荷時や全設定初期化時、本製品のDHCPサーバー機能は「しない」、IPアドレスは「192.168.0.1」に設定されています。
本製品を既存のネットワークに接続して使用する場合には、使用状況にあわせて設定を変更してください。

## HUBとの接続について

100BASE-TXより低速なHUBは、意図しない動作で通信に障害を与えるなど、通信速度低下の原因になりますので、できるだけ接続しないでください。

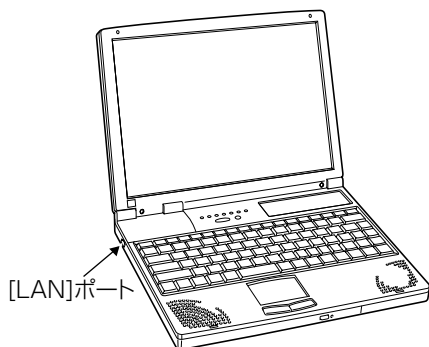
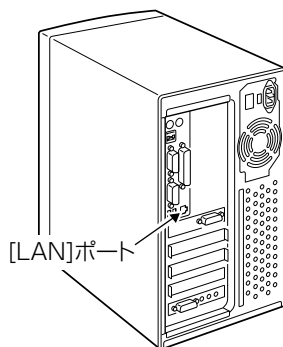
# Step1. 設定に使うパソコンの用意

**本製品の設定に使用するパソコンを用意します。**

※出荷時や全設定初期化時、本製品のIPアドレスは、「192.168.0.1」、DHCPサーバー機能（☞P54、P62）は、「しない」に設定されています。
本製品の設定画面にアクセスするときは、接続するパソコンに固定IPアドレスの設定（☞P30～P31）が必要です。

## 有線LAN端末と接続して設定する場合

LANケーブルを接続できるパソコンをご用意ください。

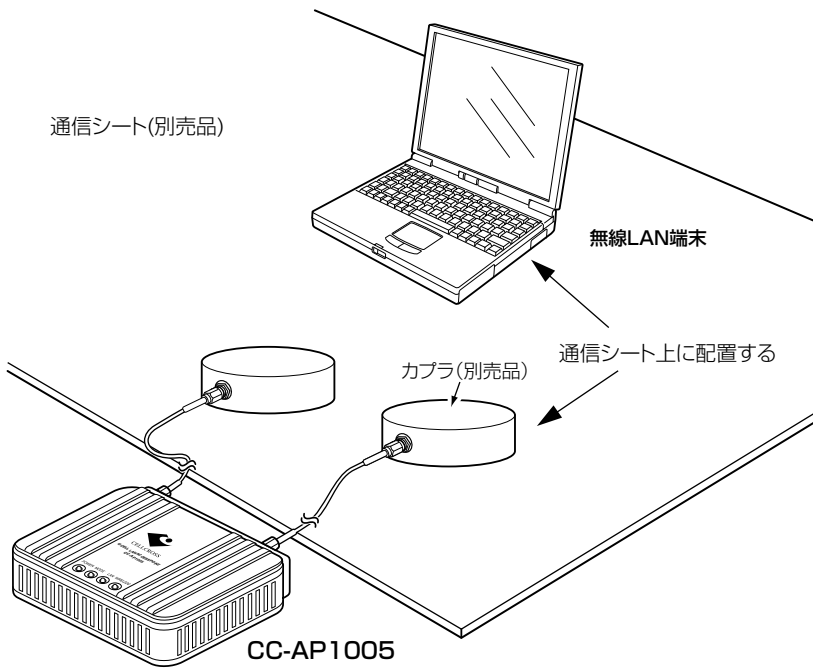
**ノートブック型パソコン**

**デスクトップ型パソコン**

※[LAN]ポートの位置は、ご使用のパソコンによって異なりますので、LANケーブルを接続するときは、パソコンの取扱説明書などでご確認ください。

※すでに有線LANでご使用のパソコンを本製品の設定に使用する場合は、そのパソコンを既存の有線LANから切りはなしてください。

## 無線LAN端末と接続して設定する場合

本製品は、[IEEE802.11n/a(W52)/b/g]規格に準拠しています。
※出荷時、本製品は、[IEEE802.11n/a]規格の無線LAN端末と通信します。

### 本製品と無線LAN端末を通信シート(ＬＡＮシート)上に配置する

※カプラと通信シート(ＬＡＮシート)が別途必要です。

## Step2. 固定IPアドレスを設定する

**本製品の設定に使用するパソコンに固定IPアドレスを設定する手順について、Windows 7を例に説明します。　　　　　　　　　　　　　　　　　　（設定例：192.168.0.100）**

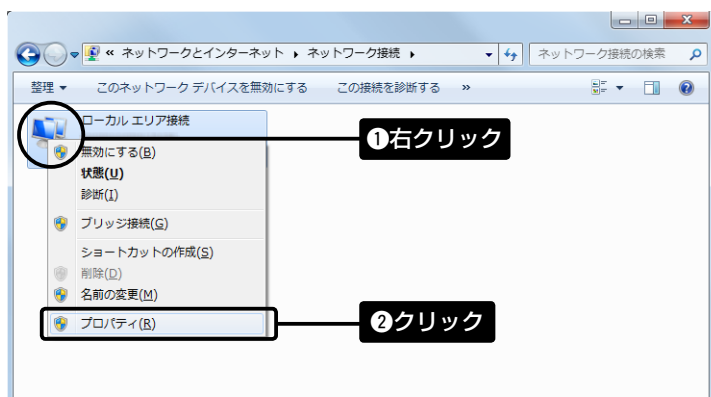
※出荷時や全設定初期化時、本製品のIPアドレスは「192.168.0.1」、DHCPサーバー機能（☞P54、P62）は「しない」に設定されています。

### Windows 7の場合

**1** マウスを〈スタート〉（ロゴボタン）→［コントロールパネル］の順に操作します。

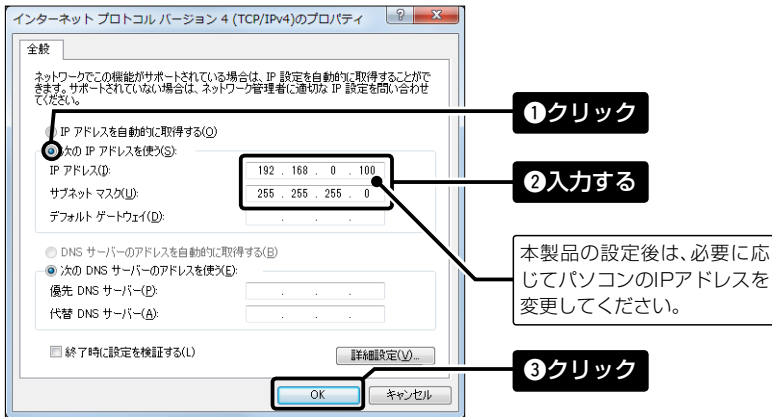
**2** コントロールパネルから、［ネットワークとインターネット］をクリックし、表示された画面で［ネットワークと共有センター］をクリックします。

**3** タスク欄の［アダプターの設定の変更］をクリックします。

**4** ［ローカルエリア接続（有線LAN端末で設定する場合）］、または［ワイヤレスネットワーク接続（無線LAN端末で設定する場合）］を右クリックし、表示されたメニューから、［プロパティ（R）］をクリックします。

**5** [ユーザーアカウント制御]のメッセージが表示された場合は、[続行]をクリックします。

**6** 「ローカル エリア接続のプロパティ」画面で、[インターネットプロトコル バージョン4(TCP/IPv4)]を選択し、〈プロパティ(R)〉をクリックします。

「インターネット プロトコル バージョン 4 (TCP/IPv4)のプロパティ」画面(別画面)を表示します。

**7** [次のIPアドレスを使う(S)]をクリックし、[IPアドレス(I)](例:192.168.0.100)と[サブネットマスク(U)](例:255.255.255.0)を入力して、〈OK〉をクリックします。

※上図は、設定例です。

**8** 「ローカル エリア接続のプロパティ」画面で、〈閉じる〉をクリックします。

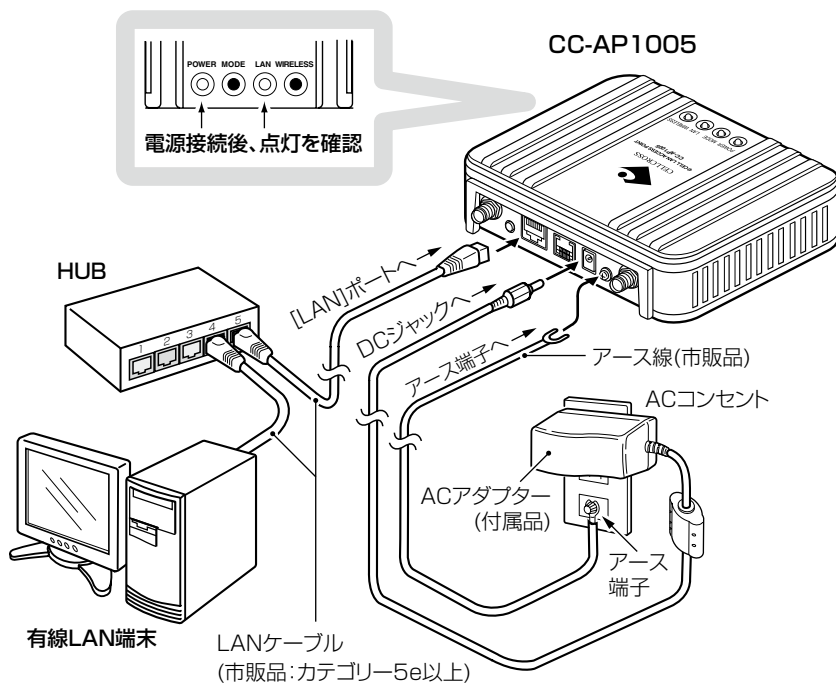
## Step3. 設定に使うパソコンの接続

本製品に接続するHUBと既存のネットワークは、切りはなして設定してください。

※本製品の[LAN]ポートは、MDI(ストレート)/MDI-X(クロス)の自動判別機能に対応しています。
HUBをお持ちでない場合でも、LANケーブルで本製品とパソコンを直接接続できます。

### 有線LAN端末を使用する場合

【ご注意】　接続するときは、本製品および接続する機器の電源を切ってください。

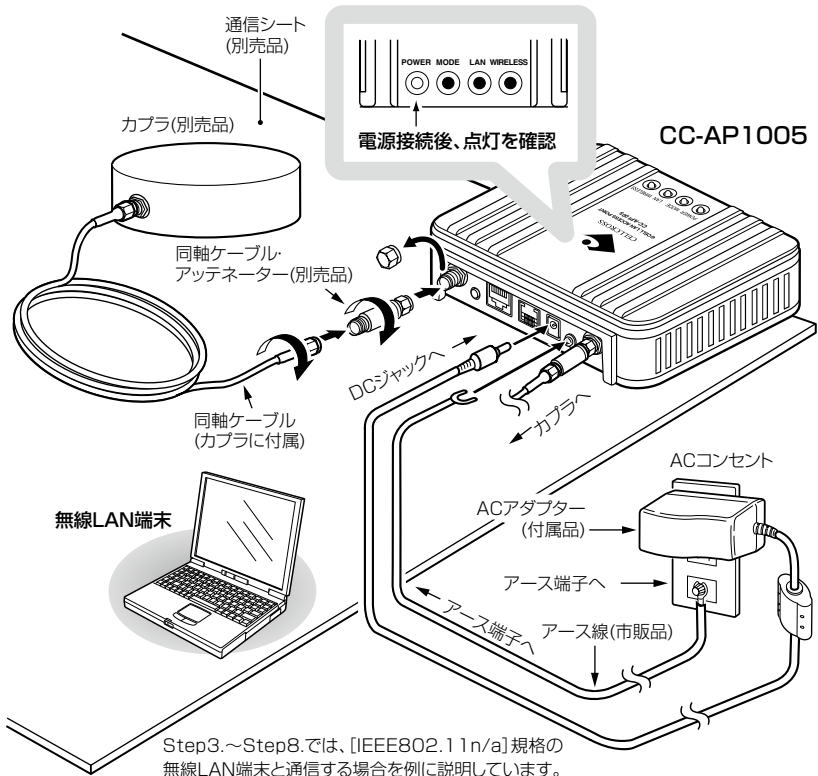
本製品とパソコン(有線LAN端末)の電源を入れます。

⚠警告　本製品のアース端子は、市販のアース線を使用して、コンセントのアース端子、または地中に埋めたアース棒(市販品)に必ず接続してください。

※落雷したときの電気的ショックの緩和、感電やノイズの回り込みを防止できます。

※絶対に、ガス管や水道管には接続しないでください。

## 無線LAN端末(Windows 7)を使用する場合

【ご注意】 接続するときは、本製品および接続する機器の電源を切ってください。

**1** カプラと無線LAN端末を通信シートの上に置いて、本製品、無線LAN端末の順番に電源を入れます。

⚠警告 本製品のアース端子は、市販のアース線を使用して、コンセントのアース端子、または地中に埋めたアース棒(市販品)に必ず接続してください。

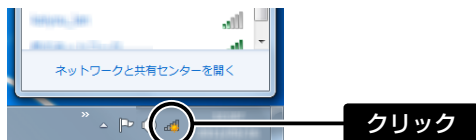
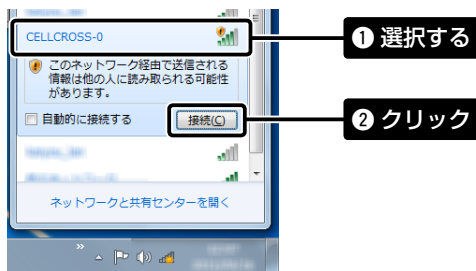
※落雷したときの電気的ショックの緩和、感電やノイズの回り込みを防止できます。

※絶対に、ガス管や水道管には接続しないでください。

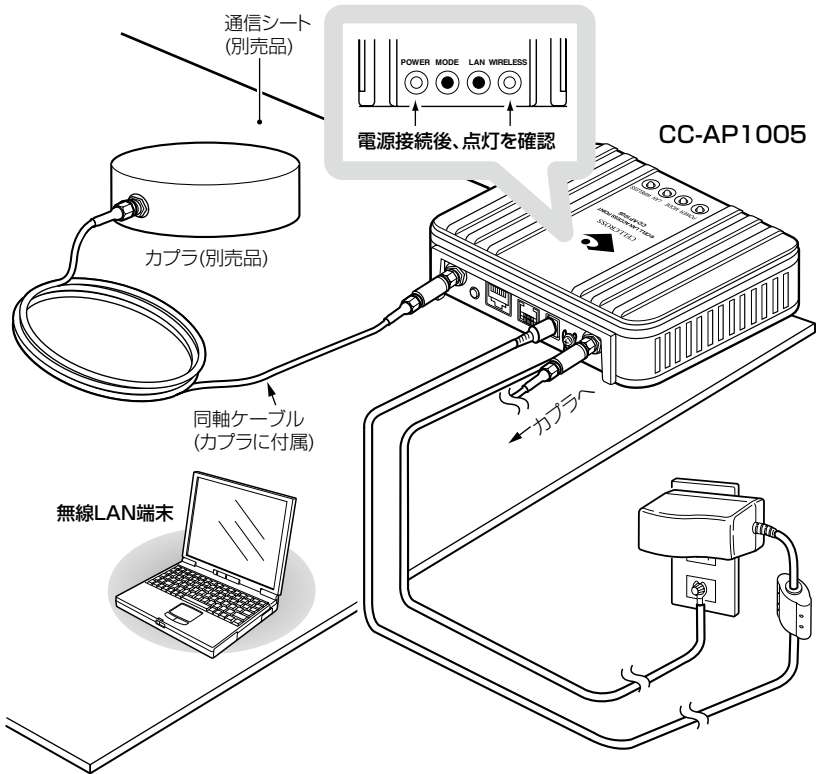
次ページにつづく➔

## Step3. 設定に使うパソコンの接続

### 無線LAN端末(Windows 7)を使用する場合

**2** [ワイヤレスネットワーク接続アイコン]をクリックします。
(環境により、下記が表示されるまで数分かかることがあります。)

**3** 本製品に設定された[SSID](出荷時の設定:CELLCROSS-0)を選択し、〈接続(C)〉をクリックして、表示される画面にしたがって操作します。

※出荷時、本製品の無線ネットワーク名(SSID)は「CELLCROSS-0」に設定されています。
※不正アクセス防止のため、必ず暗号化を設定してください。
　暗号鍵(WEPキー)/共有鍵(Pre-Shared Key)は、容易に推測されないものにしてください。
　数字とアルファベット(大文字/小文字)を組み合わせた複雑なものにし、さらに定期的に暗号鍵/共有鍵を変更すると有効です。

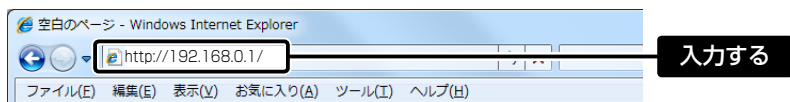
**5** 「接続」と表示されたことを確認します。

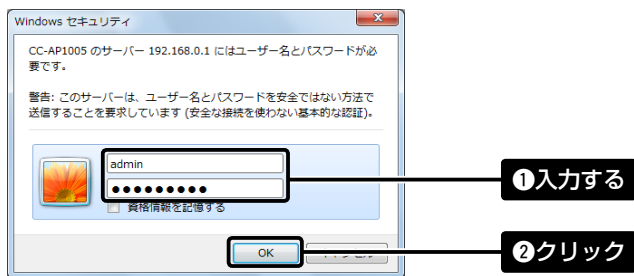
**6** 本製品の［WIRELESS］ランプが点灯したことを確認します。

## Step4. 設定画面へのアクセスを確認する

本製品に接続したパソコンのWWWブラウザーから、本製品を設定画面にアクセスする手順について説明します。

### 設定画面にアクセスするには

**1** WWWブラウザーを起動します。

**2** 本製品に設定されたIPアドレスをWWWブラウザーのアドレスバーに入力します。
出荷時、本製品のIPアドレスは「192.168.0.1」に設定されています。

**3** [Enter]キーを押します。
[ユーザー名]と[パスワード]を求める画面が表示されます。

**4** [ユーザー名]欄に「admin」、[パスワード]欄に「cellcross」(出荷時の設定)を入力し、〈OK〉をクリックすると、本製品の設定画面が表示されます。

> **WWWブラウザーについて**
> Microsoft Internet Explorer 8で動作確認しています。
> また、設定画面が正しく表示できるように、WWWブラウザーのJavaScript機能、およびCookieは有効にしてください。
> ※Microsoft Internet Explorer 7以前をご使用の場合は、正しく表示できないことがあります。

# Step5. 本体IPアドレスを変更する

本製品のIPアドレスを変更する手順について説明します。

## 設定のしかた

「ネットワーク設定」→「LAN側IP」

既存のネットワークと重複しないように設定します。

**1** 「LAN側IP」画面で、[IPアドレス設定]項目の設定を変更し、〈登録して再起動〉をクリックします。

設定が有効になります。

※IPアドレスの「ネットワーク部(例：192.168.0.)」を変更したときは、設定に使用するパソコン「ネットワーク部」についても本製品と同じに変更します。

**2** 再起動完了(約1分)後、[Back]と表示された文字の上にマウスポインターを移動してクリックします。

[ユーザー名]と[パスワード]を求める画面が表示されます。(☞P37)

### IPアドレスの割り当てかた

IPアドレスは、「ネットワーク部」と「ホスト部」の2つの要素から成り立っています。
出荷時の本製品のIPアドレス「192.168.0.1」(クラスC)を例とすると、最初の「192.168.0.」までが「ネットワーク部」で、残りの「1」を「ホスト部」といいます。
「ネットワーク部」が同じIPアドレスを持つネットワーク機器(パソコンなど)は、同じネットワーク上にあると認識されます。
さらに「ホスト部」によって同じネットワーク上にある各ネットワーク機器を識別しています。
以上のことから、IPアドレスを割り当てるときは、次のことに注意してください。

- 同じネットワークに含めたいネットワーク機器に対しては、「ネットワーク部」をすべて同じにする
- 同じネットワーク上の機器に対して、「ホスト部」を重複させない
- ネットワークアドレス(ホスト部の先頭および「0」)を割り当てない
- ブロードキャストアドレス(ホスト部の末尾および「255」)を割り当てない

## Step6. 無線ネットワーク名と暗号化を設定する(手動で設定する場合)

無線LAN端末との識別に必要なSSIDやANY接続による不正アクセス防止を設定します。
※無線ネットワーク名と暗号化を自動で設定する場合は、「Step6. 無線ネットワーク名と暗号化を設定する(自動で設定する場合)」(☞P40)をご覧ください。
※[IEEE802.11n/a]規格の無線LAN端末と通信する場合を例に説明しています。

### 無線ネットワーク名を手動で設定する

「無線設定」→「仮想AP」

- SSID　：任意に変更します。(出荷時の設定：CELLCROSS-0)
- ANY接続拒否　：[SSID]を「ANY」に設定する無線LAN端末のアクセスを禁止します。

**1** 「無線設定」メニュー、「仮想AP」の順にクリックします。
「仮想AP」画面(〈例〉インターフェース：ath0)を表示します。

**2** [仮想AP設定]項目の[SSID:]欄に、大文字/小文字の区別に注意して、任意の半角英数字32文字以内で入力します。　(入力例：CELLCROSS-0)

**3** 暗号化を手動で設定しますので、ここでは〈登録〉をクリックします。
「再起動が必要な項目が変更されています。」が表示されます。
※再起動するまで変更した設定内容は有効になりません。

#### 「ANY」での不正アクセスについて

暗号化の設定をしないで無線LAN端末をご使用の場合、無線LAN端末側がANY接続を許可するように設定されていると、本製品の[SSID]の設定に関係なく、この無線LAN端末から本製品にアクセスができます。
アクセスを拒否する場合は、上記画面で[ANY接続拒否]の設定を「する」に変更してください。
※[ANY接続拒否]の設定を「する」に変更すると、Windows標準のワイヤレスネットワーク接続画面に[SSID]が表示されなくなります。

無線LANで送受信するデータを暗号化する設定です。
※[IEEE802.11n/a]規格の無線LAN端末と通信する場合を例に説明しています。

## 暗号化を手動で設定する

「無線設定」→「仮想AP」

通信する相手の無線LAN端末にも同じ設定をしてください。

設定例） ◎ ネットワーク認証 ：「WPA-PSK･WPA2-PSK」
◎ 暗号化方式 ：「TKIP･AES」
◎ PSK（Pre-Shared Key） ：「cellcross」
※設定例以外の暗号化設定については、本書44ページ～46ページをご覧ください。

**1** [ネットワーク認証:]欄で「WPA-PSK･WPA2-PSK」を選択します。
[暗号化方式:]欄で「TKIP･AES」を選択します。
[PSK（Pre-Shared Key）:]欄で「cellcross」と半角で入力します。
※[PSK（Pre-Shared Key）:]欄に入力した文字数によって、入力モード（ASCII：半角で8文字～63文字入力/16進数：64桁入力）を自動判別します。

**2** 〈登録して再起動〉をクリックします。

**3** 再起動完了（約1分）後、[Back]と表示された文字の上にマウスポインターを移動してクリックします。

2

## 無線ネットワーク名と暗号化を設定する(自動で設定する場合)

無線ネットワーク名と暗号化を自動設定するために、WPS(Wi-Fi Protected Setup)機能を使用できるように設定します。

※無線ネットワーク名と暗号化を手動で設定する場合は、「Step6. 無線ネットワーク名と暗号化を設定する(手動で設定する場合)」(☞P38〜P39)をご覧ください。
※本製品のWPS状態が未設定表示の場合は、本製品で自動生成されたSSIDと共有鍵(キー)を無線LAN端末に自動設定します。
※[IEEE802.11n/a]規格の無線LAN端末と通信する場合を例に説明しています。

### WPS機能を有効にする

「無線設定」→「WPS」

「プッシュボタン方式」(☞P142、P143)を例に説明します。
※WPS機能を有効にすると、本製品の後面パネルにある〈WPS〉ボタンの操作が有効になります。
なお、「仮想AP」画面(〈例〉インターフェース:ath0)の暗号化設定は、無効になります。

**1** 「無線設定」メニュー、「WPS」の順にクリックします。
「WPS」画面を表示します。

**2** WPS機能を使用する仮想APを[使用するインターフェース:]欄で選択(例:ath0)して、〈登録して再起動〉の順にクリックします。
★「ath3」を選択すると、[IEEE802.11a/b/g]規格の通信になります。(☞P22)

**3** 再起動完了(約1分)後、[Back]と表示された文字の上にマウスポインターを移動してクリックします。

# 無線LANの詳細設定

# 第3章

**この章では、**
**無線LANの詳細な機能を設定する手順について説明します。**

## 1. [IEEE802.11 b /g]規格で無線通信するには

[IEEE802.11 b /g]規格の無線LAN端末を使用して、本製品と無線通信するには、次の手順でチャンネルを変更してください。

### 設定のしかた

「無線設定」→「無線LAN」

出荷時や全設定初期化時、チャンネルは「036CH(5180MHz)」に設定されています。

**1** 「無線設定」メニューをクリックします。

「無線LAN」画面を表示します。

**2** チャンネルを選択します。

**3** 〈登録して再起動〉をクリックします。

※ほかの機能も併せて設定するときは、〈登録〉をクリックします。

**4** 再起動完了(約1分)後、[Back]と表示された文字の上にマウスポインターを移動してクリックすると、設定画面に戻ります。

## 2. [WEP RC4]暗号化を設定するには

[WEP RC4]暗号化を設定する仮想の暗号鍵(キー)による設定は、次のとおりです。

- 16進数で暗号鍵(キー)を直接入力する(☞P44)
- ASCII文字で暗号鍵(キー)を直接入力する(☞P45)
- [キージェネレーター]に入力した文字列より暗号鍵(キー)を生成する(☞P46)

※ [WPA-PSK(TKIP)/(AES)]暗号化設定例については、本書39ページをご覧ください。

### 暗号鍵(キー)の入力について

[暗号化方式]の設定によって、入力する暗号鍵(キー)の文字数や桁数が異なります。
また、入力された文字数、および桁数によって、入力モード(16進数/ASCII文字)を自動判別します。

| ネットワーク認証 | 入力モード / 暗号化方式 | 16進数 (HEX) | ASCII文字 |
|---|---|---|---|
| オープンシステム/共有キー | WEP RC4 64(40)ビット | 10桁 | 5文字(半角) |
| | WEP RC4 128(104)ビット | 26桁 | 13文字(半角) |
| | WEP RC4 152(128)ビット | 32桁 | 16文字(半角) |

※入力できる桁数および文字数は、( )内のビット数に対する値です。
※無線LAN端末側で、[キーインデックス]の設定を「1」以外で使用している場合は、[キーインデックス]を「1」に変更して、そのテキストボックスに本製品と同じ暗号鍵(キー)を設定してください。

### ASCII文字→16進数変換表について

相手が指定する[入力モード]で暗号鍵(キー)を設定できない場合は、下記の変換表を参考に指示された暗号鍵(キー)に対応する記号や英数字で入力してください。
[例]16進数入力で「4153434949」(10桁)を設定している場合、ASCII文字では、「ASCII」(5文字)になります。

| ASCII文字 | | ! | ” | # | $ | % | & | ’ | ( | ) | * | + | , | - | . | / |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 16進数 | 20 | 21 | 22 | 23 | 24 | 25 | 26 | 27 | 28 | 29 | 2a | 2b | 2c | 2d | 2e | 2f |
| ASCII文字 | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | : | ; | < | = | > | ? |
| 16進数 | 30 | 31 | 32 | 33 | 34 | 35 | 36 | 37 | 38 | 39 | 3a | 3b | 3c | 3d | 3e | 3f |
| ASCII文字 | @ | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O |
| 16進数 | 40 | 41 | 42 | 43 | 44 | 45 | 46 | 47 | 48 | 49 | 4a | 4b | 4c | 4d | 4e | 4f |
| ASCII文字 | P | Q | R | S | T | U | V | W | X | Y | Z | [ | ¥ | ] | ^ | _ |
| 16進数 | 50 | 51 | 52 | 53 | 54 | 55 | 56 | 57 | 58 | 59 | 5a | 5b | 5c | 5d | 5e | 5f |
| ASCII文字 | ` | a | b | c | d | e | f | g | h | i | j | k | l | m | n | o |
| 16進数 | 60 | 61 | 62 | 63 | 64 | 65 | 66 | 67 | 68 | 69 | 6a | 6b | 6c | 6d | 6e | 6f |
| ASCII文字 | p | q | r | s | t | u | v | w | x | y | z | { | \| | } | ˜ | |
| 16進数 | 70 | 71 | 72 | 73 | 74 | 75 | 76 | 77 | 78 | 79 | 7a | 7b | 7c | 7d | 7e | |

## 2. [WEP RC4]暗号化を設定するには

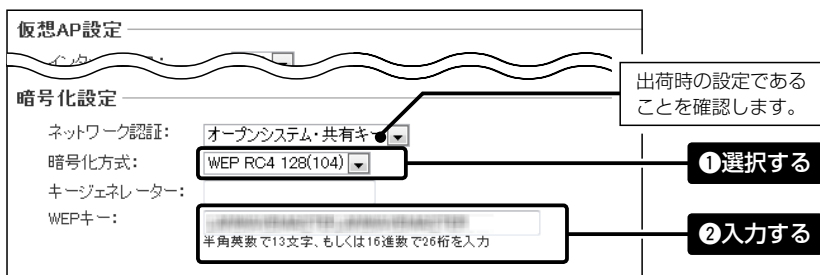
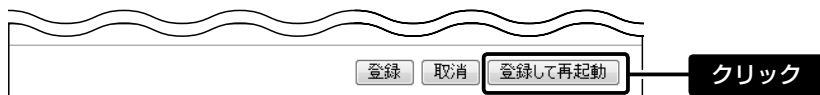
### 16進数で暗号鍵(キー)を入力するには

「無線設定」→「仮想AP」

出荷時や全設定初期化時、暗号化は設定されていません。
次の条件で設定する場合を例に説明します。

- [ネットワーク認証:] :「オープンシステム・共有キー」(出荷時の設定)
- [暗号化方式:] :「WEP RC4 128(104)」ビット
- [WEPキー:] :「0〜9」、および「a 〜f(またはA 〜F)」を使用して、26桁を入力

**1** 「無線設定」メニュー、[仮想AP]の順にクリックします。
「仮想AP」画面(〈例〉インターフェース:ath0)を表示します。

**2** [暗号化方式:]欄で「WEP RC4 128(104)」を選択し、13文字の暗号鍵(キー)を[WEPキー:]欄に入力します。

**3** 〈登録して再起動〉をクリックします。
※ほかの機能も併せて設定するときは、〈登録〉をクリックします。

**4** 再起動完了(約1分)後、[Back]と表示された文字の上にマウスポインターを移動してクリックします。

**無線LAN端末のキーインデックスについて**(Windows XP Service Pack適用時を除く)

Service Packを適用していないWindows XP標準のワイヤレスネットワーク接続を使用して本製品と[WEP RC4]で通信する場合、無線LAN端末側のキーインデックスを「0」に設定してください。
キーインデックスが「1」〜「3」に設定されているときは、本製品と通信できません。

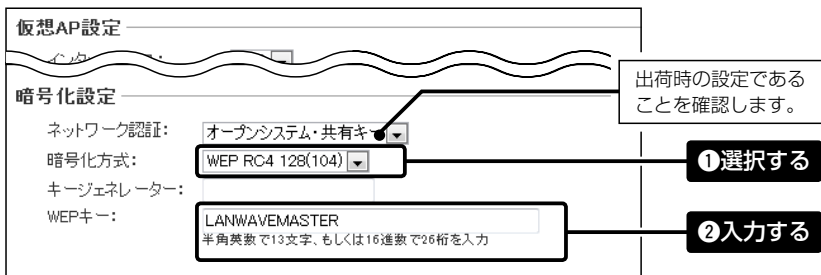
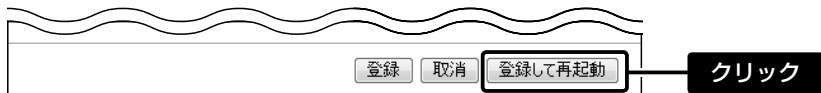
## ASCII文字で暗号鍵(キー)を入力するには

「無線設定」→「仮想AP」

出荷時や全設定初期化時、暗号化は設定されていません。
次の条件で設定する場合を例に説明します。

- [ネットワーク認証:] :「オープンシステム・共有キー」(出荷時の設定)
- [暗号化方式:] :「WEP RC4 128(104)」ビット
- [WEPキー:] :13文字を入力(例:LANWAVEMASTER)

**1** 「無線設定」メニュー、[仮想AP]の順にクリックします。
「仮想AP」画面(〈例〉インターフェース:ath0)を表示します。

**2** [暗号化方式:]欄で「WEP RC4 128(104)」を選択し、13文字の暗号鍵(キー)を[WEPキー:]欄に入力します。

**3** 〈登録して再起動〉をクリックします。
※ほかの機能も併せて設定するときは、〈登録〉をクリックします。

**4** 再起動完了(約1分)後、[Back]と表示された文字の上にマウスポインターを移動してクリックします。

3

## 2. [WEP RC4]暗号化を設定するには

### 暗号鍵(キー)を生成するには

「無線設定」→「仮想AP」

出荷時や全設定初期化時、暗号化は設定されていません。
次の条件で設定する場合を例に説明します。

- [ネットワーク認証:] :「オープンシステム・共有キー」(出荷時の設定)
- [暗号化方式:] :「WEP RC4 128(104)」ビット
- [キージェネレーター:] :任意の文字列(半角英数字31文字以内)を入力(例:cellcross)

**1** 「無線設定」メニュー、[仮想AP]の順にクリックします。
「仮想AP」画面(〈例〉インターフェース:ath0)を表示します。

**2** [暗号化方式:]欄で「WEP RC4 128(104)」を選択し、任意の文字列を[キージェネレーター:]欄に入力(例:cellcross)します。

**3** 〈登録して再起動〉をクリックします。
※ほかの機能も併せて設定するときは、〈登録〉をクリックします。

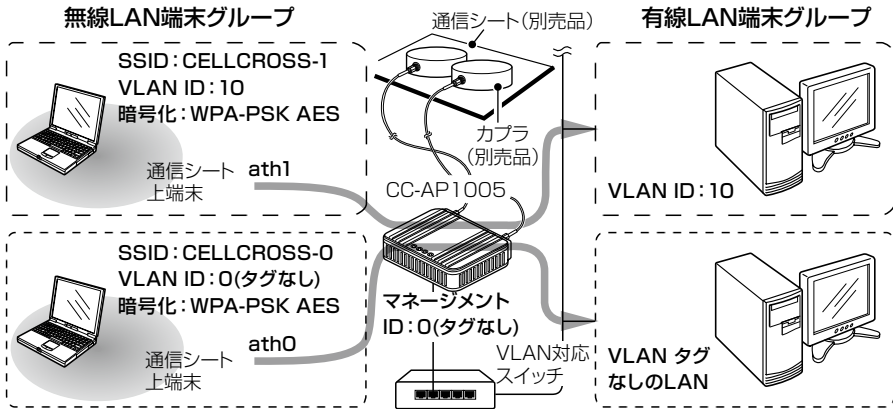
**4** 再起動完了(約1分)後、[Back]と表示された文字の上にマウスポインターを移動してクリックします。

#### キージェネレーターについて

◎ 任意の文字列を入力すると、「16進数」の暗号鍵(キー)が[WEPキー:]欄のテキストボックスに自動生成されます。
◎ [WEPキー:]欄のテキストボックスに生成される桁数および文字数は、選択する[暗号化方式]によって異なります。
**※キージェネレーターは、弊社およびアイコム社製以外の機器と互換性はありません。**

# 3. 仮想APを設定するには

下図の仮想AP無線VLANグループを構成するための設定手順を説明します。

※[SSID]を「CELLCROSS-0」に設定する無線LAN端末グループは、設定されているものとします。

## 設定のしかた

「無線設定」→「仮想AP」

上図の　　色で示す無線LAN端末について、次の条件を設定する例を説明します。
操作手順は、次ページで説明しています。

| | | |
|---|---|---|
| ● [仮想AP設定]項目 | [インターフェース:] | :「ath1」 |
| | [仮想APを使用:] | :「する」 |
| | [SSID:] | :「CELLCROSS-1」(出荷時の設定) |
| | [VLAN ID:] | :「10」 |
| ● [暗号化設定:]項目 | [ネットワーク認証:] | :「WPA-PSK」 |
| | [暗号化方式:] | :「AES」 |
| | [PSK(Pre-Shared Key):] | :「LANWAVEMASTER」 |

次ページにつづく➔

## 3. 仮想APを設定するには

**1** 「無線設定」メニュー、[仮想AP]の順にクリックします。

「仮想AP」画面(〈例〉インターフェース:ath0)を表示します。

**2** [インターフェース:]欄で「ath1」を選択し、前ページの設定条件にしたがって下記のように設定します。

**3** 〈登録して再起動〉をクリックします。

※ほかの機能も併せて設定するときは、〈登録〉をクリックします。

**4** 再起動完了(約1分)後、[Back]と表示された文字の上にマウスポインターを移動してクリックします。

# 4. MACアドレスフィルタリングを設定するには

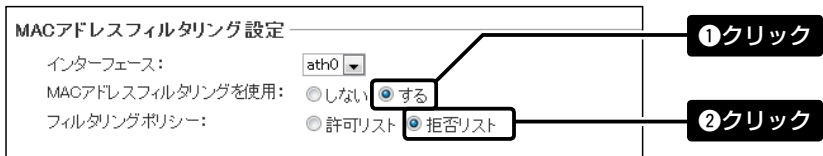
無線LAN端末のMACアドレスを登録する手順について説明します。
仮想AP(ath0～ath3)ごとに、異なる無線LAN端末を登録できます。

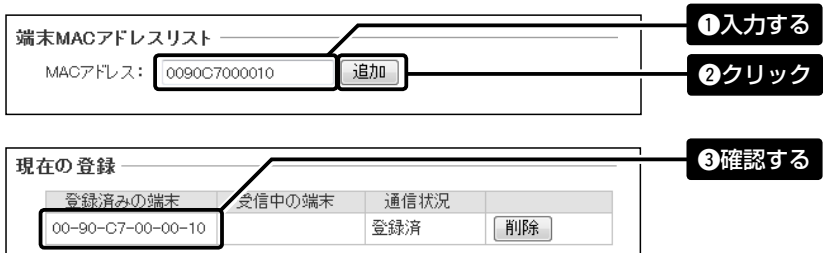
## 設定のしかた

「無線設定」→「MACアドレスフィルタリング」

本製品への接続を拒否する無線LAN端末の登録例を説明します。

**1** 「無線設定」メニュー、[MACアドレスフィルタリング]の順にクリックします。
「MACアドレスフィルタリング」画面(〈例〉インターフェース:ath0)を表示します。

**2** [MACアドレスフィルタリングを使用:]欄で「する」、[フィルタリングポリシー:]欄で「拒否リスト」の順にクリックします。

**3** 〈登録〉をクリックします。
※〈登録して再起動〉をクリックした場合でも、本製品の再起動なしに設定内容が反映されます。

**4** 接続拒否として登録する無線LAN端末のMACアドレスを[MACアドレス:]欄に入力し、〈追加〉をクリックします。
入力したMACアドレスが[現在の登録]項目に表示されます。

※[現在の登録]項目の各欄についての説明は、本書133ページをご覧ください。

# そのほかの基本設定

# 第４章

**この章では、**
**そのほかに設定が必要と思われる機能について説明しています。**

## 1. 設定画面へのアクセスを制限するには

設定者用の[管理者パスワード]を設定することで、管理者以外がWWWブラウザーから本製品の設定を変更できないようにします。

### 設定のしかた

「システム設定」→「管理者」

出荷時、本製品の設定画面には、[管理者ID(admin)]と[パスワード(cellcross)]でアクセスできます。

**1** 「システム設定」メニューをクリックします。
「管理者」画面を表示します。

**2** [現在のパスワード]欄、[新しいパスワード]欄、[新しいパスワード再入力]欄に、任意の英数字(半角31文字以内)で大文字/小文字の区別に注意して入力します。
入力した文字は、すべて「*(アスタリスク)」、または「●(黒丸)」で表示されます。

**3** 〈登録〉をクリックします。
※〈登録して再起動〉をクリックした場合でも、本製品の再起動なしに設定内容が反映されます。

**4** [ユーザー名]と[パスワード]を求める画面が表示されますので、設定した[管理者パスワード]を入力します。
本製品の設定画面を表示します。

**【不正アクセス防止のアドバイス】**
本製品に設定するすべてのパスワードは、容易に推測されないものにしてください。
数字だけでなくアルファベット(大文字/小文字)や記号などを組み合わせた長く複雑なものにし、さらに定期的にパスワードを変更すると有効です。

**【ご注意】**
管理者パスワードを忘れた場合、設定を確認できなくなりますのでご注意ください。
※お忘れの場合、本製品の〈MODE〉ボタンを本書172ページの操作にしたがい、設定を工場出荷時(初期化)の状態に戻していただくことになります。

## 2. 内部時計を設定するには

本製品の内部時計を設定する手順について説明します。

※本製品の自動時計設定機能を使用する場合についても記載していますので、併せてご覧ください。

### 設定のしかた

「システム設定」➔「時計」

本製品の内部時計を正確に表示させるため、設定されることをおすすめします。

**1** 「システム設定」メニュー、[時計]の順にクリックします。

「時計」画面を表示します。

**2** パソコンから自動取得した時刻が[内部時計設定]項目に表示されていることを確認し、〈時刻設定〉をクリックします。

内部時計に設定された時刻が、[本体の時刻]欄に表示されます。

※[設定する時刻]欄に表示されている時刻がパソコンと異なるときは、はじめからやりなおすと正確な時刻を取得できます。

※「時計」画面の〈登録〉では、時刻を設定できません。

※初期に参照しているNTPサーバーは、インターネットマルチフィード株式会社のものです。
http://www.jst.mfeed.ad.jp/

**【ご注意】**

本製品の電源を切ると、本製品の内部時計の設定が出荷時の状態に戻ります。
本製品の自動時計設定機能を使用しない場合は、停電や不慮の事故で電源が一時的に切れたときでも、内部時計の再設定が必要になります。
また、自動時計設定機能は、NTPサーバーへの問い合わせ先(経路)を設定する必要があります。
経路を設定しないときは、問い合わせできません。
「ネットワーク設定」メニュー→「LAN側IP」画面→[IPアドレス設定]項目にある[デフォルトゲートウェイ:]欄、または「ルーティング」画面の[スタティックルーティング設定]項目で、ルーティングテーブルを設定してください。

## 3. 本製品のDHCPサーバー機能を使用するには

有線LANおよび無線LANで本製品のDHCPサーバー機能を使用するときは、下記の手順でDHCPサーバー機能と自動割り当て開始IPアドレスを設定してください。

※本製品を接続するネットワーク上にDHCPサーバーが存在する場合に使用すると、IPアドレスの競合など、ネットワーク障害の原因になりますのでご注意ください。

### 設定のしかた

「ネットワーク設定」→「DHCPサーバー」

**1** 「ネットワーク設定」メニュー、[DHCPサーバー]の順にクリックします。

「DHCPサーバー」画面を表示します。

**2** [DHCPサーバー設定] 項目で、[DHCPサーバー機能を使用:] 欄の「する」をクリックし、必要に応じて[割り当て開始IPアドレス]などを変更します。

**3** 〈登録して再起動〉をクリックします。

※ほかの機能も併せて設定するときは、〈登録〉をクリックします。

**4** 設定後、本製品のDHCPサーバーからIPアドレスを自動的に取得できるように、接続するパソコンのIPアドレス設定を変更し、設定画面にアクセスします。

[ユーザー名]と[パスワード]を求める画面が表示されます。

# 設定画面について

# 第5章

**この章では、**
**各メニューで表示される設定画面について説明します。**

---



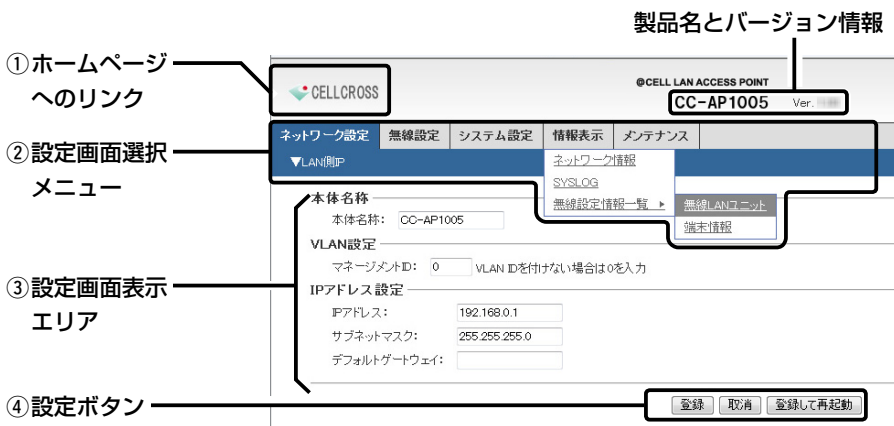
**【ご参考に】**

設定画面は、各メニューとして用途ごとに分類されていますので、「設定画面の構成について」(☞P184～P185)と併せてご覧ください。
「メンテナンス」メニューについては、「保守について」(☞6章)で、操作方法と併せて説明しています。

下記は、前ページからの「つづき」です。

下記は、前ページからの「つづき」です。

## 1. 設定画面の名称と機能

本製品の設定画面の名称と各画面に含まれる項目を説明します。
設定画面の構成について詳しくは、本書184ページ〜185ページをご覧ください。

### ①ホームページへのリンク

インターネットに接続できる環境で、アイコンをクリックすると、弊社のホームページを閲覧できます。

### ②設定画面選択メニュー

各メニューのタイトル上にマウスポインターを合わせると、そのメニューに含まれる画面名称(例:ネットワーク情報/SYSLOG/無線設定情報一覧)を表示します。
※階層のあるメニューには、▶印が表示されています。

### ③設定画面表示エリア

[設定画面選択メニュー]で選択したメニューに含まれる画面名称(例:ネットワーク情報/SYSLOG)をクリックしたとき、その画面の内容を表示します。

### ④設定ボタン

設定した内容の登録や取り消しをします。
〈登録〉をクリックして、「再起動が必要な項目が変更されています。」と表示されるときは、〈登録して再起動〉をクリックすると、画面上で確定された内容が有効になります。
再起動中は、下記の画面を表示します。

| 本体を再起動しています。<br>本体の起動を確認後、[Back]をクリックしてください。 |
|---|

※再起動が完了(約1分)するまで、[Back]と表示された文字の上にマウスポインターを移動してクリックしても、設定画面に戻りませんので、しばらくしてから再度クリックしてください。
※表示画面によって、表示されるボタンの種類や位置が異なります。

# 2. 「LAN側IP」画面

## ■ 本体名称

「ネットワーク設定」－「LAN側IP」

本製品の名称を設定します。

本体名称

本体名称： CC-AP1005

**本体名称：** ………………… 「Telnet」で本製品に接続したとき、ここで設定した本体名称を表示します。　（出荷時の設定：CC-AP1005）
※アルファベットではじまる半角英数字（a ～ z 、A ～Z、0～9、－）を、31文字以内で設定します。
なお、それ以外の文字は、登録できない場合があります。
※「－（ハイフン）」を本体名称の先頭、または末尾に使用すると、登録できません。

## ■ VLAN設定

「ネットワーク設定」－「LAN側IP」

VLAN機能についての設定です。

VLAN設定

マネージメントID： 0 VLAN IDを付けない場合は0を入力

**マネージメントID：** …… 本製品に設定された同じID番号を持つネットワーク上の機器からのアクセスだけを許可できます。
（出荷時の設定：0）
設定できる範囲は、「0～4094」です。
※VLAN IDを使用しないネットワークから本製品にアクセスするときは、「0」を設定します。
※不用意に設定すると、本製品の設定画面にアクセスできなくなりますのでご注意ください。

## 2.「LAN側IP」画面

### ■ IPアドレス設定

「ネットワーク設定」ー**「LAN側IP」**

本製品のLAN側IPアドレスを設定します。

| IPアドレス設定 | |
|---|---|
| ① IPアドレス： | 192.168.0.1 |
| ② サブネットマスク： | 255.255.255.0 |
| ③ デフォルトゲートウェイ： | |

**①IPアドレス：** ………… 本製品のIPアドレスを設定します。

（出荷時の設定：192.168.0.1）

本製品を現在稼働中のネットワークに接続するときなど、そのLANに合わせたネットワークアドレスに変更してください。

※本製品のDHCPサーバー機能を使用する場合は、「DHCPサーバー」画面にある［DHCPサーバー設定］項目の［割り当て開始IPアドレス］欄（☞P60、P68）についてもネットワーク部を同じ設定にしてください。

**②サブネットマスク：**

………………………… 本製品のサブネットマスク（同じネットワークで使用するIPアドレスの範囲）を設定します。

（出荷時の設定：255.255.255.0）

本製品を現在稼働中のネットワークに接続するときなど、そのLANに合わせたサブネットマスクに変更してください。

**【例：「255.255.255.248」に設定する場合】**

同じネットワークで使用するIPアドレスの範囲は、「192.168.0.0～192.168.0.7」になります。

この場合、端末に割り当てできるIPアドレスの範囲は、「192.168.0.2～192.168.0.6」です。

なお、端末に割り当てできないIPアドレスは次のようになります。

「192.168.0.0」：ネットワークアドレス
「192.168.0.1」：本製品のLAN側IPアドレス
「192.168.0.7」：ブロードキャストアドレス

③デフォルトゲートウェイ：

………………………… 本製品のIPアドレスとネットワーク部が異なる接続先と通信する場合、パケット転送先機器のIPアドレスを入力します。
※本製品と同じIPアドレスは、登録できません。

## 3.「DHCPサーバー」画面

### ■ DHCPサーバー設定

「ネットワーク設定」ー「DHCPサーバー」

DHCPサーバー機能についての設定です。

| DHCPサーバー設定 | |
|---|---|
| ① DHCPサーバー機能を使用: | ○しない ◉する |
| ② 割り当て開始IPアドレス: | 192.168.0.10 |
| ③ 割り当て個数: | 30 個 |
| ④ サブネットマスク: | 255.255.255.0 |
| ⑤ リース期間: | 72 時間 |
| ⑥ ドメイン名: | |
| ⑦ デフォルトゲートウェイ: | |
| ⑧ プライマリーDNSサーバー: | |
| ⑨ セカンダリーDNSサーバー: | |
| ⑩ プライマリーWINSサーバー: | |
| ⑪ セカンダリーWINSサーバー: | |

**① DHCPサーバー機能を使用:**

………………………… DHCPサーバー機能の使用を設定します。
（出荷時の設定：しない）
「する」に設定すると、② ～ ⑪の設定が有効になり、本製品に有線および無線で接続している端末がTCP/IP設定を「IPアドレスを自動的に取得する」にしている場合、本製品のDHCPクライアントになります。

**② 割り当て開始IPアドレス:**

………………………… 本製品に有線および無線で接続する端末へ、IPアドレスを自動で割り当てるときの開始アドレスを設定します。
（出荷時の設定：192.168.0.10）

③ **割り当て個数:** ……… 本製品が自動割り当てできるIPアドレスの個数を設定します。 (出荷時の設定:30)
[割り当て開始IPアドレス](②)欄に設定されたIPアドレスから連続で自動割り当てできるIPアドレスの最大個数は、0〜128(無線LANで接続する端末を含む)までです。
※128個を超える分については設定できませんので、手動でクライアントに割り当ててください。
※「0」を設定したときは、自動割り当てをしません。

④ **サブネットマスク:**
……………………… [割り当て開始IPアドレス](②)欄に設定されたIPアドレスに対するサブネットマスクです。
(出荷時の設定:255.255.255.0)

⑤ **リース期間:** ………… DHCPサーバーが割り当てるIPアドレスの有効期間を時間で指定します。 (出荷時の設定:72)
設定できる範囲は、「1〜9999(時間)」です。

⑥ **ドメイン名:** ………… 指定のドメイン名を設定する必要があるときは、DHCPサーバーが有線で接続する端末に通知するネットワークアドレスのドメイン名を127文字(半角英数字)以内で入力します。

⑦ **デフォルトゲートウェイ:**
……………………… [割り当て開始IPアドレス](②)欄のIPアドレスとネットワーク部が異なる接続先と通信する場合、パケット転送先機器のIPアドレスを入力します。

⑧ **プライマリーDNSサーバー:**
……………………… DNSサーバーのアドレスが2つある場合は、優先したい方のアドレスを入力します。
入力すると、設定したDNSサーバーアドレスをDHCPクライアントに通知します。

## 3.「DHCPサーバー」画面

### ■ DHCPサーバー設定

「ネットワーク設定」ー**「DHCPサーバー」**

| DHCPサーバー設定 | |
|---|---|
| ① DHCPサーバー機能を使用: | ○しない ◉する |
| ② 割り当て開始IPアドレス: | 192.168.0.10 |
| ③ 割り当て個数: | 30 個 |
| ④ サブネットマスク: | 255.255.255.0 |
| ⑤ リース期間: | 72 時間 |
| ⑥ ドメイン名: | |
| ⑦ デフォルトゲートウェイ: | |
| ⑧ プライマリーDNSサーバー: | |
| ⑨ セカンダリーDNSサーバー: | |
| ⑩ プライマリーWINSサーバー: | |
| ⑪ セカンダリーWINSサーバー: | |

**⑨ セカンダリーDNSサーバー:**

………………………… [プライマリーDNSサーバー]（⑧）欄と同様に、DNSサーバーのアドレスが2つある場合は、DNSサーバーアドレスのもう一方を入力します。

**⑩ プライマリーWINSサーバー:**

………………………… WINSサーバーを利用する場合は、WINSサーバーアドレスを入力します。
WINSサーバーのアドレスが2つある場合は、優先したい方のアドレスを入力します。

**⑪ セカンダリーWINSサーバー:**

………………………… 「プライマリーWINSサーバー」と同様、WINSサーバーのアドレスが2つある場合は、残りの一方を入力します。

## ■ 静的DHCPサーバー設定

「ネットワーク設定」ー「DHCPサーバー」

固定IPアドレスを特定の端末に割り当てる設定です。

**静的DHCPサーバー設定**

| MACアドレス | IPアドレス | |
|---|---|---|
| 0090c7 | 192.168.0.50 | 追加 |

※画面の値は、入力例です。

**静的DHCPサーバー設定**

………………………… 端末のMACアドレスとIPアドレスの組み合わせを登録します。

※本製品のDHCPサーバー機能(☞P54、P62)を使用する場合に有効です。

※入力後は、〈追加〉をクリックしてください。

※最大32個の組み合わせまで登録できます。

登録する端末のIPアドレスは、DHCPサーバー機能による割り当て範囲および本製品のIPアドレスと重複しないように指定してください。

## ■ 現在の登録

「ネットワーク設定」ー「DHCPサーバー」

[静的DHCPサーバー設定]項目で登録した内容を表示します。

**現在の登録**

| MACアドレス | IPアドレス | |
|---|---|---|
| 00-90-C7- | 192.168.0.50 | 削除 |

※画面の値は、登録例です。

**〈削除〉**……………………… 登録した内容を取り消すときは、該当する欄の〈削除〉をクリックします。

5

# 4.「ルーティング」画面

## ■ IP経路情報

「ネットワーク設定」－**「ルーティング」**

パケットの送信において、そのパケットをどのルーター、またはどの端末に配送すべきかの情報を表示します。

**IP経路情報**

| ①宛先 | ②サブネットマスク | ③ゲートウェイ | ④経路 | ⑤作成 |
|---|---|---|---|---|
| 127.0.0.0 | 255.0.0.0 | 127.0.0.1 | lo0 | misc |
| 127.0.0.1 | 255.255.255.255 | 127.0.0.1 | lo0 | host |
| 192.168.0.0 | 255.255.255.0 | 192.168.0.2 | mirror0 | misc |

※この項目には、現在有効な経路だけを表示します。

①**宛先** …………………… ルーティングの対象となるパケットの宛先IPアドレスを表示します。

②**サブネットマスク**…… ルーティングの対象となるパケットの宛先IPアドレスに対するサブネットマスクを表示します。

③**ゲートウェイ** ………… ルーティングの対象となるパケットの宛先IPアドレスに対するゲートウェイを表示します。

④**経路** …………………… ルーティングの対象となるパケットの宛先IPアドレスに対する転送先インターフェースを表示します。

◎lo0　　　:ループバックアドレスを意味するインターフェース

◎mirror0 :インターフェースが本機自身の場合

⑤**作成** …………………… どのように経路情報が作成されたかを表示します。

◎static　:スタティック(定義された)ルートにより作成

◎misc　　:ブロードキャストに関係するフレーム処理で作成

◎host　　:ホストルートにより作成

## ■ スタティックルーティング設定

「ネットワーク設定」ー「ルーティング」

パケットの中継経路を最大32件まで登録できます。

スタティックルーティング設定

| ①宛先 | ②サブネットマスク | ③ゲートウェイ | ④ |
|---|---|---|---|
| 192.168.1.0 | 255.255.255.0 | 192.168.0.11 | 追加 |

※画面の値は、入力例です。

① **宛先** …………………… 対象となる相手先のIPアドレスを入力します。

② **サブネットマスク** …… 対象となる宛先のIPアドレスに対するサブネットマスクを入力します。

③ **ゲートウェイ** ………… パケット転送先ルーターのIPアドレスを入力します。

④ **〈追加〉** ………………… 入力内容が登録され、[現在の登録]項目に表示します。

## ■ 現在の登録

「ネットワーク設定」ー「ルーティング」

[スタティックルーティング設定]項目で登録した内容を表示します。

現在の登録

| 宛先 | サブネットマスク | ゲートウェイ | |
|---|---|---|---|
| 192.168.1.0 | 255.255.255.0 | 192.168.0.11 | 削除 |

※画面の値は、登録例です。

**〈削除〉**…………………… 登録した内容を取り消すときは、該当する欄の〈削除〉をクリックします。

# 5.「パケットフィルター」画面

## ■ パケットフィルター

「ネットワーク設定」ー**「パケットフィルター」**

登録したエントリーに該当するパケットを通過させたり、通過を阻止させたりするフィルターの設定です。

パケットフィルター

① 番号:
② このエントリーを使用: しない する
③ ログを表示: しない する
④ 方法: 遮断 透過
インターフェース
⑤ 送信元インターフェース: すべて
⑥ 宛先インターフェース: すべて
Ethernet フレームパラメーター
⑦ 送信元MACアドレス/マスク:
⑧ 宛先MACアドレス/マスク:
⑨ VLAN ID: ～ VLAN IDを付けない場合は0を入力
⑩ Ethernetタイプ: すべて 0x

①**番号:** …………………… フィルターを比較する順位を指定します。
設定できる範囲は、「1～64」です。
本製品が受信、または送信するパケットと[現在の登録]項目に表示されたフィルターと比較します。
※フィルタリングの条件は、1つ以上指定してください。
※番号が指定されていないときは、登録できません。
※IPv6のパケットには対応していません。

**【順位と比較について】**
フィルターを複数設定しているときは、番号の小さい順番に比較を開始します。
フィルタリングの条件に一致した中から、番号が最小のエントリーで処理をします。
※フィルタリングの条件に一致した時点で、それ以降の識別番号のエントリーは比較しません。

②**このエントリーを使用：**

…………………………　登録するフィルターの使用について設定します。

（出荷時の設定：しない）

登録だけして使用しないときは、「しない」を選択します。

③**ログを表示：**…………　「情報表示」メニューの「SYSLOG」画面へのログ表示について設定します。（出荷時の設定：する）

④**方法：**…………………　フィルタリングの方法を選択します。

（出荷時の設定：透過）

◎遮断：すべてのフィルタリング条件に一致した場合、そのパケットを破棄します。

◎透過：すべてのフィルタリング条件に一致した場合、そのパケットを通過します。

⑤**送信元インターフェース：**

…………………………　フィルタリングの対象となる送信元インターフェースを選択します。（出荷時の設定：すべて）

◎mirror0　：インターフェースが本機自身の場合

◎ag0　：インターフェースが有線LANの場合

◎ath0～ath3：インターフェースが本製品の無線LAN（仮想AP）の場合

※「すべて」を選択すると、「mirror0」、「ag0」、「ath0～ath3」が送信元インターフェースの対象になります。

⑥**宛先インターフェース：**

…………………………　フィルタリングの対象となる宛先インターフェースを選択します。（出荷時の設定：すべて）

◎mirror0　：インターフェースが本機自身の場合

◎ag0　：インターフェースが有線LANの場合

◎ath0～ath3：インターフェースが本製品の無線LAN（仮想AP）の場合

※「すべて」を選択すると、「mirror0」、「ag0」、「ath0～ath3」が宛先インターフェースの対象になります。

## 5.「パケットフィルター」画面

### ■ パケットフィルター

「ネットワーク設定」ー**「パケットフィルター」**

パケットフィルター

① 番号:

② このエントリーを使用: しない する

③ ログを表示: しない する

④ 方法: 遮断 透過

インターフェース

⑤ 送信元インターフェース: すべて

⑥ 宛先インターフェース: すべて

Ethernet フレームパラメーター

⑦ 送信元MACアドレス／マスク:

⑧ 宛先MACアドレス／マスク:

⑨ VLAN ID: ～ VLAN IDを付けない場合は0を入力

⑩ Ethernetタイプ: すべて 0x

**⑦送信元MACアドレス／マスク:**

フィルタリングの対象となるEthernetヘッダー内において、送信元MACアドレスの有効範囲を設定します。
フィルタリングの条件として、これらを2進数で表現したときの論理積(AND)が[現在の登録]項目(☞P83)に表示されます。
※登録例については、[宛先MACアドレス／マスク:](⑧)欄で説明しています。

**⑧宛先MACアドレス／マスク:**

フィルタリングの対象となるEthernetヘッダー内において、宛先MACアドレスの有効範囲を設定します。
フィルタリングの条件として、これらを2進数で表現したときの論理積(AND)が[現在の登録]項目(☞P83)に表示されます。

⑧宛先MACアドレス／マスク：（つづき）

**【MACアドレスとマスク値の登録例】**

［送信元MACアドレス／マスク：］（⑦）欄についても、下記の例を参考にしてください。

※小文字で入力しても、登録結果は、登録例（例1.～例3.）のように大文字になります。

**例1.）** 宛先MACアドレス/マスク
00-90-C7-3C-00-64/（空白）
［現在の登録］項目（☞P89）には、下記の内容で表示します。
00-90-C7-3C-00-64/FF-FF-FF-FF-FF-FF
※マスクを指定しないときは、「FF-FF-FF-FF-FF-FF」として登録されます。
※00-90-C7-3C-00-64に一致するMACアドレスがフィルタリングの対象になります。

**例2.）** 宛先MACアドレス/マスク
00-90-C7-3C-00-64/FF-FF-FF-00-00-00
［現在の登録］項目（☞P89）には、下記の内容で表示します。
00-90-C7-00-00-00/FF-FF-FF-00-00-00
※マスク値「0」との論理積は、「0」になるため、「00-90-C7」部分が一致するMACアドレスがフィルタリング対象になります。

## 5.「パケットフィルター」画面

### ■ パケットフィルター

「ネットワーク設定」－**「パケットフィルター」**

パケットフィルター
① 番号：
② このエントリーを使用： しない する
③ ログを表示： しない する
④ 方法： 遮断 透過
インターフェース
⑤ 送信元インターフェース： すべて
⑥ 宛先インターフェース： すべて
Ethernet フレームパラメーター
⑦ 送信元MACアドレス／マスク：
⑧ 宛先MACアドレス／マスク：
⑨ VLAN ID： ～ VLAN IDを付けない場合は0を入力
⑩ Ethernetタイプ： すべて 0x

⑧宛先MACアドレス／マスク：

…………………………【MACアドレスとマスク値の登録例】（つづき）

**例3.）** 宛先MACアドレス/マスク
00-90-C7-3C-00-64/FF-FF-FF-00-00-FF
［現在の登録］項目（☞P89）には、下記の内容で表示します。
00-90-C7-00-00-64/FF-FF-FF-00-00-FF
※00-90-C7-00-00-64～00-90-C7-FF-FF-64までが有効範囲になります。
例2.と同様、マスク「00」の部分は、どんな値のMACアドレスでもフィルタリングの条件に一致する対象となります。

⑨VLAN ID: ………… フィルタリングの対象となる[VLAN ID]を指定(開始値～終端値)します。
入力できる範囲は、「0～4094」です。
「0」を開始値に指定したときは、範囲指定できません。
※開始値だけを設定したときは、一致するパケットが対象です。
※「0」は、VLANタグのないパケット、およびVLAN IDが「0」のパケットが対象です。
「0」以外は、指定のVLANタグ付きパケットが対象です。

⑩Ethernetタイプ: ……フィルタリングの対象となるEthernetタイプ名称(ARP/IP)、または16進数(0000～ffff〈4桁〉)で指定します。 (出荷時の設定:すべて)
※16進数で指定するとき、小文字(例:ffff)で入力しても、登録結果は大文字(例:FFFF)になります。

## 5.「パケットフィルター」画面

### ■ パケットフィルター

「ネットワーク設定」―**「パケットフィルター」**

[Ethernetタイプ:](⑩)欄で、「ARP」を選択したときは、下記の画面になります。

| | | | |
|---|---|---|---|
| ⑩Ethernetタイプ: | ARP | 0x | |
| ARP パラメーター | | | |
| ⑪ARPタイプ: | すべて | | |
| ⑫送信元MACアドレス/マスク: | | | |
| ⑬送信元IPアドレス: | | ~ | |
| ⑭ターゲットMACアドレス/マスク: | | | |
| ⑮ターゲットIPアドレス: | | ~ | |

**⑪ARPタイプ:**………… フィルタリングの対象となるARPタイプを選択します。
(出荷時の設定:すべて)
「すべて」、「request」、「reply」、「rrequest」、「rreply」から選択できます。
※「すべて」を選択すると、すべてのARPタイプに該当します。

**⑫送信元MACアドレス/マスク:**
……………………… フィルターの対象となるARPヘッダー内において、送信元MACアドレスの有効範囲を設定します。
フィルタリングの条件として、これらを2進数で表現したときの論理積(AND)が[現在の登録]項目(☞P83)に表示されます。
※登録例については、[宛先MACアドレス/マスク:](⑧)欄で説明しています。

⑬ **送信元IPアドレス:**

…………………………　フィルターの対象となるARPヘッダー内において、送信元IPアドレスの有効範囲(開始値〜終端値)を設定します。

◎開始値だけを設定したときは、開始値と一致したときフィルタリングします。

◎終端値だけを設定したときは、「0.0.0.0」から終端値までの範囲をフィルタリングします。

⑭ **ターゲットMACアドレス/マスク:**

…………………………　フィルターの対象となるARPヘッダー内において、ターゲットMACアドレスの有効範囲を設定します。

フィルタリングの条件として、これらを2進数で表現したときの論理積(AND)が[現在の登録]項目(☞P83)に表示されます。

※登録例については、[宛先MACアドレス/マスク:](⑧)欄で説明しています。

⑮ **ターゲットIPアドレス:**

…………………………　フィルターの対象となるARPヘッダー内において、ターゲットIPアドレスの有効範囲(開始値〜終端値)を設定します。

◎開始値だけを設定したときは、開始値と一致したときフィルタリングします。

◎終端値だけを設定したときは、「0.0.0.0」から終端値までの範囲をフィルタリングします。

## 5.「パケットフィルター」画面

### ■ パケットフィルター

「ネットワーク設定」－**「パケットフィルター」**

［Ethernetタイプ:］（⑩）欄で「IP」を選択、［IPプロトコル:］（⑬）欄で「すべて」/「指定」を選択したときは、下記の画面になります。

| | |
|---|---|
| ⑩ Ethernetタイプ： | IP ▼ 0x |
| IPv4 パラメーター | |
| ⑪ 送信元IPアドレス： | ～ |
| ⑫ 宛先IPアドレス： | ～ |
| ⑬ IPプロトコル： | すべて ▼ |

**⑪ 送信元IPアドレス：**
…………………………フィルターの対象となるIPヘッダー内において、送信元IPアドレスの有効範囲(開始値～終端値)を設定します。
◎開始値だけを設定したときは、開始値と一致したときフィルタリングします。
◎終端値だけを設定したときは、「0.0.0.0」から終端値までの範囲をフィルタリングします。
※IPv6には対応していません。

**⑫ 宛先IPアドレス：**……フィルターの対象となるIPヘッダー内において、宛先IPアドレスの有効範囲(開始値～終端値)を設定します。
◎開始値だけを設定したときは、開始値と一致したときフィルタリングします。
◎終端値だけを設定したときは、「0.0.0.0」から終端値までの範囲をフィルタリングします。
※IPv6には対応していません。

⑬ **IPプロトコル:** ……… フィルターの対象となるIPヘッダー内において、パケットのトランスポート層プロトコルを選択します。

◎すべて :すべてのプロトコルに一致します。
◎ICMP :ICMPだけに一致します。
◎IGMP :IGMPだけに一致します。
◎TCP :TCPだけに一致します。
◎UDP :UDPだけに一致します。
◎指定 :右のテキストボックスに、IPヘッダーに含まれるパケットのトランスポート層プロトコル番号を入力します。
プロトコル番号は、10進数で0～255までの半角数字を入力します。

## 5.「パケットフィルター」画面

### ■ パケットフィルター

「ネットワーク設定」―**「パケットフィルター」**

[Ethernetタイプ:](⑩)欄で「IP」を選択、[IPプロトコル:](⑬)欄で「ICMP」を選択したときは、下記の画面になります。

| | |
|---|---|
| ⑩ Ethernetタイプ: | IP 0x |
| IPv4 パラメーター | |
| ⑪ 送信元IPアドレス: | ～ |
| ⑫ 宛先IPアドレス: | ～ |
| ⑬ IPプロトコル: | ICMP |
| ⑭ タイプ: | |
| ⑮ コード: | |

**⑭ タイプ:** ………………… フィルタリングの対象となるICMPヘッダー内のタイプを番号(0～255)で指定します。
下記は、代表的なタイプです。

| | | |
|---|---|---|
| [0] echorep | [9] routerad | [14] timestrep |
| [3] unreach | [10] routersel | [15] inforeq |
| [4] squench | [11] timex | [16] inforep |
| [5] redir | [12] paramprob | [17] maskreq |
| [8] echo | [13] timest | [18] maskrep |

※選択したタイプは、[現在の登録]項目の該当する欄に上記の数字で表示します。
※指定しないときは、すべてがフィルタリングの対象になります。

**⑮ コード:** ………………… フィルタリングの対象となるICMPヘッダー内のコードを番号(0～255)で指定します。
※割り当てのない番号を指定、または番号を指定しないときは、すべてがフィルタリングの対象になります。

## ■ パケットフィルター

「ネットワーク設定」―**「パケットフィルター」**

[Ethernetタイプ:](⑩)欄で「IP」を選択、[IPプロトコル:](⑬)欄で「IGMP」を選択したときは、下記の画面になります。

| | | |
|---|---|---|
| ⑩ Ethernetタイプ: | IP ▼ 0x | |
| IPv4 パラメーター | | |
| ⑪ 送信元IPアドレス: | | ~ |
| ⑫ 宛先IPアドレス: | | ~ |
| ⑬ IPプロトコル: | IGMP ▼ | |
| ⑭ タイプ: | 0x | |
| ⑮ グループアドレス: | | ~ |

⑭ **タイプ:** ………………… フィルタリングの対象となるIGMPヘッダー内のタイプを16進数(00~ff〈2桁〉)で指定します。
※指定しないときは、すべてがフィルタリングの対象になります。

⑮ **グループアドレス:**
………………………… フィルタリングの対象となるIGMPヘッダー内のマルチキャストグループアドレスの有効範囲(開始値~終端値)を設定します。
◎開始値だけを設定したときは、開始値と一致したときフィルタリングします。
◎終端値だけを設定したときは、「0.0.0.0」から終端値までの範囲をフィルタリングします。
※IPv6には対応していません。

## ■ パケットフィルター

「ネットワーク設定」―**「パケットフィルター」**

[Ethernetタイプ:](⑩)欄で「IP」を選択、[IPプロトコル:](⑬)欄で「TCP」を選択したときは、下記の画面になります。

| | |
|---|---|
| ⑩ Ethernetタイプ: | IP 0x |
| IPv4 パラメーター | |
| ⑪ 送信元IPアドレス: | ～ |
| ⑫ 宛先IPアドレス: | ～ |
| ⑬ IPプロトコル: | TCP |
| ⑭ 送信元ポート: | ～ |
| ⑮ 宛先ポート: | ～ |
| ⑯ TCPフラグ: | □URG □ACK □PSH □RST □SYN □FIN |

**⑭送信元ポート:** ……… フィルタリングの対象となる送信元TCPポート番号(1～65535)の有効範囲(開始値～終端値)を指定します。
◎開始値だけを設定したときは、開始値と一致したときフィルタリングします。
◎終端値だけを設定したときは、「1」から終端値までの範囲をフィルタリングします。
◎送信元ポートを指定しないときは、すべてのTCPポート番号がフィルタリングの対象になります。
※TCPヘッダー内のSource Portと比較します。

**⑮宛先ポート:** ………… フィルタリングの対象となる宛先TCPポート番号(1～65535)の有効範囲(開始値～終端値)を指定します。
◎開始値だけを設定したときは、開始値と一致したときフィルタリングします。
◎終端値だけを設定したときは、「1」から終端値までの範囲をフィルタリングします。
◎宛先ポートを指定しないときは、すべてのTCPポート番号がフィルタリングの対象になります。
※TCPヘッダー内の、Destination Portと比較します。

⑯TCPフラグ：………… フィルタリングの対象となるTCPフラグを指定します。
※本製品で指定できるフラグは、URG、ACK、PSH、RST、SYN、FINです。
※TCPヘッダー内のTCPフラグと比較します。
※選択したフラグは、[現在の登録]項目に表示されます。
※何も指定しない場合は、TCPフラグの状態に関係なくフィルタリングの対象になります。
※複数のフラグを選択した場合は、複数のフラグが同時に立っているパケットをフィルタリング対象とします。

## 5.「パケットフィルター」画面

### ■ パケットフィルター

「ネットワーク設定」－**「パケットフィルター」**

[Ethernetタイプ:](⑩)欄で「IP」を選択、[IPプロトコル:](⑬)欄で「UDP」を選択したときは、下記の画面になります。

| | | |
|---|---|---|
| ⑩ Ethernetタイプ: | IP ▼ 0x | |
| IPv4 パラメーター | | |
| ⑪ 送信元IPアドレス: | ～ | |
| ⑫ 宛先IPアドレス: | ～ | |
| ⑬ IPプロトコル: | UDP ▼ | |
| ⑭ 送信元ポート: | ～ | |
| ⑮ 宛先ポート: | ～ | |

⑭**送信元ポート:** ……… フィルタリングの対象となる送信元UDPポート番号(1～65535)の有効範囲(開始値～終端値)を指定します。
◎開始値だけを設定したときは、開始値と一致したときフィルタリングします。
◎終端値だけを設定したときは、「1」から終端値までの範囲をフィルタリングします。
◎送信元ポートを指定しないときは、すべてのUDPポート番号がフィルタリングの対象になります。
※UDPヘッダー内のSource Portと比較します。

⑮**宛先ポート:** ………… フィルタリングの対象となる宛先UDPポート番号(1～65535)の有効範囲(開始値～終端値)を指定します。
◎開始値だけを設定したときは、開始値と一致したときフィルタリングします。
◎終端値だけを設定したときは、「1」から終端値までの範囲をフィルタリングします。
◎宛先ポートを指定しないときは、すべてのUDPポート番号がフィルタリングの対象になります。
※UDPヘッダー内の、Destination Portと比較します。

## ■ 現在の登録

「ネットワーク設定」－「パケットフィルター」

[パケットフィルター]項目から登録した現在の各エントリーの内容を表示します。

現在の 登録

| 番号 | 1 | 〈編集〉〈削除〉 |
|---|---|---|
| このエントリーを使用 | する | |
| ログを表示 | しない | |
| 方法 | 透過 | |
| 送信元インターフェース | すべて | |
| 宛先インターフェース | すべて | |
| 送信元MACアドレス／マスク | 00-90-C7-[illegible]／FF-FF-FF-[illegible] | |
| 宛先MACアドレス／マスク | 00-90-C7-[illegible]／FF-FF-FF-[illegible] | |
| VLAN ID | 0 | |
| Ethernetタイプ | IP | |
| 送信元IPアドレス | − | |
| 宛先IPアドレス | − | |
| IPプロトコル | TCP | |
| 送信元ポート | − | |
| 宛先ポート | − | |
| TCPフラグ | − | |

※上記画面の内容は、登録例です。
※未設定の項目には、「-」が表示されます。

**〈編集〉**……………………… 左の欄に表示されたエントリーを編集するボタンです。
〈編集〉をクリックすると、その左の欄に表示された内容を[パケットフィルター]項目(☞P68)の各欄に表示します。

**〈削除〉**……………………… 左の欄に表示されたエントリーを削除するボタンです。
〈削除〉をクリックすると、削除されます。

## 5.「パケットフィルター」画面

### ■ パケットフィルター使用例

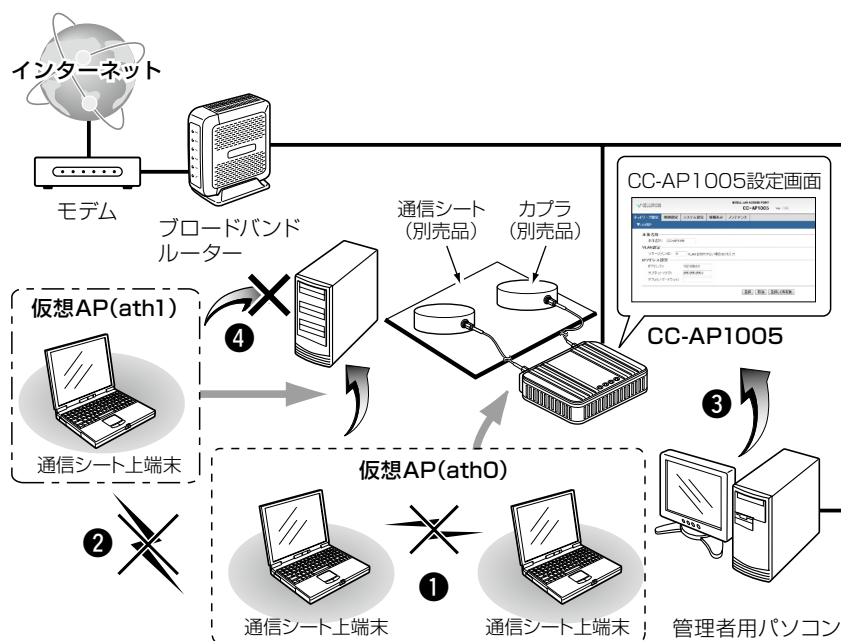
「ネットワーク設定」－「パケットフィルター」

下図とその説明(❶～❹)に示すような使用例について、パケットフィルターの設定方法を説明します。

❶ 仮想AP(ath0:VLAN IDなし)内の無線LAN端末同士の通信を禁止するには (☞P85)

❷ 仮想AP(ath0:VLAN IDなしとath1:VLAN IDなし)間の無線LAN端末同士の通信を禁止するには (☞P86)

❸ CC-AP1005の設定画面へのアクセスを管理者用端末に制限するには (☞P87～P88)

❹ 仮想AP(ath1:VLAN IDなし)からインターネットへの接続を許可し、有線LAN(ファイルサーバーなど)への接続を禁止するには (☞P89)

※各仮想APグループのパソコン(3台)は、通信シートの上に置かれているものとします。

## ■ パケットフィルター使用例

「ネットワーク設定」ー「パケットフィルター」

前ページに示す(❶～❹)について、設定例を説明します。

❶ 仮想AP(ath0：VLAN IDなし)内の無線LAN端末同士の通信を禁止するには
送信元インターフェース、宛先インターフェースともにath0を設定することによりath0に接続した無線端末間通信禁止ができます。
また、MACアドレスを指定しない場合、ath0に接続するすべての無線端末が遮断条件に該当します。

現在の登録

| 番号 | |
|---|---|
| このエントリーを使用 | する |
| ログを表示 | |
| 方法 | 遮断 |
| 送信元インターフェース | ath0 |
| 宛先インターフェース | ath0 |
| 送信元MACアドレス／マスク | – |
| 宛先MACアドレス／マスク | – |
| VLAN ID | 0 |
| Ethernetタイプ | すべて |



次ページにつづく➔

## 5.「パケットフィルター」画面

### ■ パケットフィルター使用例

「ネットワーク設定」―「パケットフィルター」

❷仮想AP(ath0:VLAN IDなしとath1:VLAN IDなし)間の無線LAN端末同士の通信を禁止するには

下記の2つ(1.と2.)のフィルターの登録が必要です。

## ■ パケットフィルター使用例

「ネットワーク設定」―「**パケットフィルター**」

❸CC-AP1005の設定画面へのアクセスを管理者用端末に制限するには

※マネージメントIDが「0」の場合を例に説明しています。

※設定に使用する端末からのWEB画面へのアクセスを妨げないようエントリー追加・削除の順番は、注意してください。
エントリーを追加するときは、透過エントリー→遮断エントリーの順に、エントリーの削除は、遮断エントリー→透過エントリーの順に操作してください。

下記の2つ(1.と2.)のフィルターの登録が必要です。
※設定例については、次ページをご覧ください。

**1.**管理用端末からのWEBアクセスを透過
**2.**管理用端末以外からのWEBアクセスを遮断

次ページにつづく➔

## 5. 「パケットフィルター」画面

### ■ パケットフィルター使用例

「ネットワーク設定」―「パケットフィルター」

❸CC-AP1005の設定画面へのアクセスを管理者用端末に制限するには(つづき)

下記の2つ(1.と2.)のフィルターの登録が必要です。

## ■ パケットフィルター使用例

「ネットワーク設定」ー「**パケットフィルター**」

❹ 仮想AP（ath1：VLAN IDなし）からインターネットへの接続を許可し、有線LAN（ファイルサーバーなど）への接続を禁止するには

※ブロードバンドルーター以外のDHCPサーバーを使用する場合は、対応する透過エントリーを追加してください。

下記の2つ（1.と2.）のフィルターの登録が必要です。

# 6.「無線LAN」画面

## ■ 無線LAN設定

「無線設定」－「無線LAN」

本製品に内蔵された無線LANカードに対する設定です。

**無線LAN設定**

① 無線UNITを使用： ○しない ◉する
② チャンネル： 011CH (2462 MHz) ☐40MHz帯域幅モード
③ パワーレベル： -5dB
④ ストリーム数（Tx×Rx）： 2×2
⑤ 最低レート制限： 36 Mbps
⑥ DTIM間隔： 1
⑦ プロテクション機能： ○無効 ◉有効

**①無線UNITを使用：**

……………………… 無線通信機能の使用を設定します。

（出荷時の設定：する）

「しない」に設定すると、本製品の無線通信機能を停止します。

また、「する」に設定されているときだけ、下記の内容を「情報表示」メニューにある「ネットワーク情報」画面の[無線LANユニット]項目（☞P160）に表示します。

**無線LANユニット**

| インターフェース | SSID | BSSID |
|---|---|---|
| ath0 | CELLCROSS-0 | 00-90-C7- |

②チャンネル: ………… 本製品の無線通信に使用するチャンネルを設定します。
（出荷時の設定：036CH（5180MHz）、
□ 40MHz帯域幅モード）

無線LAN端末は、本製品のチャンネルを自動的に検知して通信します。

**☑ 40MHz帯域幅モード：**
チェックボックスにチェックマークを入れると、通常（20MHz）の２倍の周波数帯域幅を使用して、最大300Mbps（理論値）の速度で通信します。

**□ 40MHz帯域幅モード：**（20MHz帯域幅モード）
チェックボックスのチェックマークをはずしたときは、従来と同じ周波数帯域幅（20MHz）を使用して、最大130Mbps（理論値）の速度で通信します。

下記のように、選択するチャンネルによって、使用できる無線LAN規格が異なります。

「001CH」～「013CH」を選択すると、
［IEEE802.11n/b/g］規格〈2.4GHz帯〉で通信します。
⇒本書92ページをご覧ください。

「036CH」～「048CH」を選択すると、
［IEEE802.11n/a（W52）］規格〈5.2GHz帯〉で通信します。
⇒本書94ページをご覧ください。

次ページにつづく➔

## 6.「無線LAN」画面

### ■ 無線LAN設定

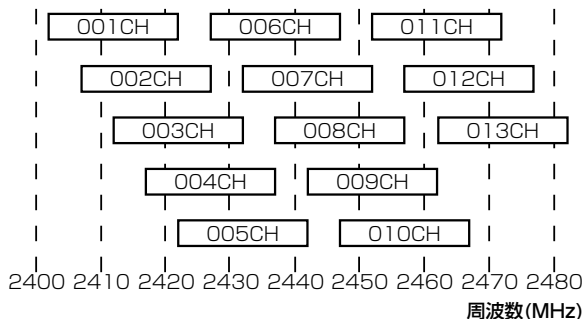
「無線設定」―**「無線LAN」**

②チャンネル:(つづき)

◎**[IEEE802.11n/b/g]規格について**

**「20MHz帯域幅モード」**(☞P91)で使用する場合、下図に示すように、帯域の1部が重複するため、近くに[IEEE802.11n/b/g]規格の無線アクセスポイントやビル間通信機器が存在するときは、電波干渉することがあります。

電波干渉を防止するため、本製品の「チャンネル」は、別の無線ネットワークグループと4チャンネル以上空けて設定してください。

たとえば、お互いの設定を、「001CH(2412MHz)」-「006CH(2437MHz)」-「011CH(2462MHz)」にすると電波干渉しません。

②チャンネル: ………… ◎[IEEE802.11n/b/g]規格について　　　　(つづき)

**「40MHz帯域幅モード」**で(☞P91)使用する場合、下図に示すように、2倍の周波数帯域幅(40MHz)の電波を使用するため、「010CH(2457MHz)~013CH(2472MHz)」は設定できません。

さらに、帯域の1部がすべてのチャンネルで重複するため、近くに[IEEE802.11n/b/g]規格で異なるチャンネルの無線アクセスポイントやビル間通信機器が存在するときは、電波干渉することがあります。

電波干渉を防止するときは、20MHz帯域幅モード(☞P91)に変更するか、[パワーレベル](☞P95)、または機器の設置場所を変更してください。

次ページにつづく➔

## 6.「無線LAN」画面

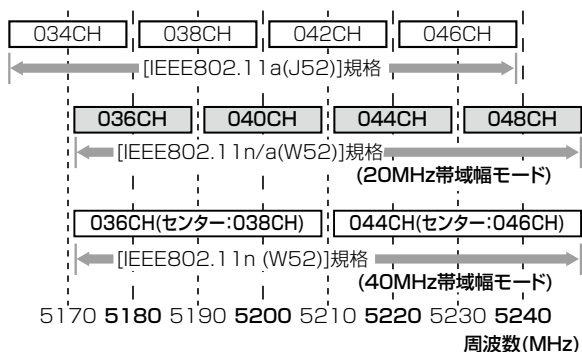
### ■ 無線LAN設定

「無線設定」—**「無線LAN」**

②チャンネル:(つづき)

**◎[IEEE802.11n/a(W52)]規格について**

近くに[IEEE802.11a(J52)]規格で無線LAN端末が稼働しているとき、本製品の[IEEE802.11n/a(W52)]規格の「036CH(5180MHz)〜048CH(5240MHz)」をご使用になると、下図に示すように電波干渉の原因になることがありますのでご注意ください。

※**「40MHz帯域幅モード」**で(☞P91)使用する場合、下図に示すように、2倍の周波数帯域幅(40MHz)の電波を使用するため、「040CH(5200MHz)」と「048CH(5240MHz)」は設定できません。

②チャンネル: ………… ◎[IEEE802.11n/a(W52)]規格について(つづき)

※[IEEE802.11a(J52)]規格は、電波法改正(2005年5月)以前の規格のため、本製品では使用できません。

※[IEEE802.11n/a(W52)]規格で通信する場合、お互いを異なるチャンネルに設定すれば、チャンネル間の電波干渉に配慮する必要はありません。

③**パワーレベル:** ……… 本製品に内蔵された無線LANカードの送信出力を設定します。

0dB/−1dB/−2dB/−3dB/−4dB/−5dBの 中(6段階)から選択できます。 (出荷時の設定:−5dB)

本製品のパワーレベルが「−5dB」の場合、最も伝送距離が短くなります。

パワーレベルを高くすると、電波強度が大きくなり、通信シート近傍以外でも通信できる場合があります。

また同一チャンネルで使用する通信シートが隣にある場合、隣の通信シートに干渉を及ぼすおそれがありますのでご注意ください。

**【パワーレベルを低くする目的について】**

◎本製品(通信シートを含む)からの電波漏洩を極力小さくしたい場合

◎通信エリアを通信シート近傍に限定してセキュリティーを高めたいとき

**【パワーレベルを高くする目的について】**

◎無線LAN端末で受信できる電波強度を大きくしたい場合

◎他の電子製品が発するノイズによる影響を軽減したい場合

## 6.「無線LAN」画面

### ■ 無線LAN設定

「無線設定」ー**「無線LAN」**

**無線LAN設定**

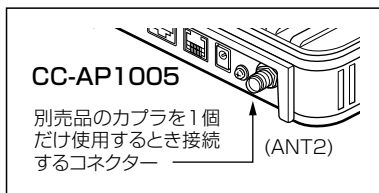
| | | |
|---|---|---|
| ① | 無線UNITを使用： | ○しない ◉する |
| ② | チャンネル： | 011CH (2462 MHz) ▼<br>☐ 40MHz帯域幅モード |
| ③ | パワーレベル： | −5dB ▼ |
| ④ | ストリーム数（Tx×Rx）： | 2×2 ▼ |
| ⑤ | 最低レート制限： | 36 Mbps ▼ |
| ⑥ | DTIM間隔： | 1 |
| ⑦ | プロテクション機能： | ○無効 ◉有効 |

**④ストリーム数(Tx×Rx)：**

…………………………… 本製品で使用するストリーム数を設定します。

（出荷時の設定：2×2）

「1×1」に設定したときは、別売品のカプラを本製品のアンテナコネクター(ANT2側)に1個だけ接続します。

ANT2側のアンテナコネクターは、本製品を後面パネルから見たとき、右側にあります。

※[ストリーム数(Tx×Rx)]は、間違った設定をすると十分な性能が得られません。
取り扱いについては、十分にご注意ください。

⑤**最低レート制限：** … 本製品の通信速度を制限するときに使用する最低レートを設定します。 （出荷時の設定：36Mbps）
無線LAN端末が対応していないレートを設定すると、本製品と接続できなくなりますので、ご使用の環境に応じて設定してください。

**【例1：「58.5Mbps～300Mbps」に設定する場合】**
[IEEE802.11n]規格の通信速度を最低レートに設定すると、仮想APの設定により、本製品と接続できる無線LAN端末が制限されます。
必要に応じて、ご使用になる仮想APの設定内容を変更してください。
※「ath0～ath2」の仮想APの暗号化方式を「なし」または「AES」に設定すると、[IEEE802.11n]規格の通信になるため、「58.5Mbps～300Mbps」に設定すると、[IEEE802.11a/b/g]規格の無線LAN端末は本製品と接続できません。
※「ath3」の仮想APは、[IEEE802.11a/b/g]規格の通信に限定されるため、「58.5Mbps～300Mbps」に設定すると、どの無線LAN端末も本製品と接続できません。

**【例2：「54Mbps」に設定する場合】**
[IEEE802.11b]規格の無線LAN端末は本製品と接続できません。

次ページにつづく➔

## 6.「無線LAN」画面

### ■ 無線LAN設定

「無線設定」―**「無線LAN」**

無線LAN設定

① 無線UNITを使用：　○しない ◉する

② チャンネル：　011CH (2462 MHz)　□40MHz帯域幅モード

③ パワーレベル：　-5dB

④ ストリーム数 (Tx×Rx)：　2×2

⑤ 最低レート制限：　36 Mbps

⑥ DTIM間隔：　1

⑦ プロテクション機能：　○無効 ◉有効

⑤最低レート制限：(つづき)

**【選択できる最低レートについて】**

選択したチャンネルや[40MHz帯域幅モード](☞P91)、[ストリーム数(Tx×Rx):]欄(☞P96)の設定により、選択できる最低レートは次のように異なります。

**20MHz帯域幅モード**　　(単位：Mbps)

「001CH」～「013CH」を選択した場合

| なし | 2 | 5.5 | 6.5 | 11 | 12 | 13 | 18 |
|---|---|---|---|---|---|---|---|
| 19.5 | 24 | 26 | 36 | 39 | 48 | 52 | 54 |
| 78 | 104 | 117 | 130 | | | | |

「036CH」～「048CH」を選択した場合

| なし | 6.5 | 9 | 12 | 13 | 18 | 19.5 | 24 |
|---|---|---|---|---|---|---|---|
| 26 | 36 | 39 | 48 | 52 | 54 | 58.5 | 65 |
| 78 | 104 | 117 | 130 | | | | |

※[ストリーム数(Tx×Rx):]欄を「1×1」にしたときは、「78Mbps ～130Mbps」(■部分のレート)を選択できません。
ただし、「001CH」～「013CH」を選択している場合は、「58.5Mbps」、「65Mbps」が選択できます。

⑤最低レート制限:(つづき)

………………………… **40MHz帯域幅モード** (単位:Mbps)

「001CH」~「009CH」を選択した場合

| なし | 2 | 5.5 | 6.5 | 11 | 12 | 13 | 13.5 |
|---|---|---|---|---|---|---|---|
| 18 | 19.5 | 24 | 27 | 36 | 39 | 40.5 | 48 |
| 52 | 54 | 58.5 | 81 | 108 | 121.5 | 135 | 150 |
| 162 | 216 | 243 | 270 | 300 | | | |

「036CH」/「044CH」を選択した場合

| なし | 6.5 | 9 | 12 | 13 | 13.5 | 18 | 19.5 |
|---|---|---|---|---|---|---|---|
| 24 | 26 | 27 | 36 | 39 | 40.5 | 48 | 52 |
| 54 | 58.5 | 65 | 78 | 81 | 108 | 121.5 | 135 |
| 150 | 162 | 216 | 243 | 270 | 300 | | |

※[ストリーム数(Tx×Rx):]欄を「1×1」にしたときは、「162Mbps ~300Mbps」(■部分のレート)を選択できません。

⑥**DTIM間隔:** ………… DTIM(Delivery Traffic Indication Message)をビーコンに挿入する間隔を設定します。 (出荷時の設定:1)
設定できる範囲は、「1~50」です。
DTIMとは、パワーセーブしている端末に対して、ブロードキャスト・マルチキャストパケット配送を伝えるメッセージのことです。
※設定を変更すると、正常に通信できないことがありますので、特に必要がない場合は、工場出荷時の状態でご使用ください。

⑦**プロテクション機能:**

………………………… 異なる無線LAN規格の混在による電波干渉をなくして、無線LANの通信速度低下を軽減したいとき有効な設定です。 (出荷時の設定:有効)
※「有効」に設定すると、[IEEE802.11n/a(W52)/b/g]規格の通信速度低下を防止でき、極端に通信速度が遅い場合に効果があります。
※接続する無線LAN端末が少ない場合、または周囲にほかの無線LAN機器が存在しない場合には、「無効」に設定してください。

5

## 7.「仮想AP」画面

### ■ 仮想AP設定

「無線設定」－「仮想AP」

本製品1台で複数の仮想無線アクセスポイントとして使用するための設定です。

| 仮想AP設定 | |
|---|---|
| ① インターフェース： | ath0 |
| ② 仮想APを使用： | ○しない ◉する |
| ③ SSID： | CELLCROSS-0 |
| ④ VLAN ID： | 0　VLAN IDを付けない場合は0を入力 |
| ⑤ ANY接続拒否： | ◉しない ○する |
| ⑥ 接続端末制限： | 63 |
| ⑦ アカウンティングを使用： | ◉しない ○する |

①インターフェース：

………………………… 設定する仮想AP(アクセスポイント)の名称(ath0～ath3)を選択します。　(出荷時の設定：ath0)
選択するインターフェースごとに、[仮想AP設定]項目(②～⑦)と[暗号化設定]項目(☞P104)の設定内容を変更できます。
※仮想APの名称(ath0～ath3)は、変更できません。
※「ath1～ath3」を使用するときは、[仮想APを使用](②)欄(☞P101)の設定を「する」に変更してください。
※「MACアドレスフィルタリング」画面(☞P49、P124)についても、仮想APごとに設定できます。
※ご使用のWWWブラウザーでJavaScript®が「無効」に設定されていると、仮想APの名称を選択したとき、[仮想AP設定]項目(②～⑦)と[暗号化設定]項目(☞P104)の設定内容が更新されません。
更新されないときは、ご使用のWWWブラウザーでJavaScript®の設定が「有効」に設定されていることを確認してください。

②仮想APを使用：…… ［インターフェース］（①）欄で選択した仮想AP（ath0～ath3）の使用について設定します。
（出荷時の設定：ath0選択時→する
ath1選択時→しない
ath2選択時→しない
ath3選択時→しない）
※「ath0」は、設定を「しない」に変更できません。
※通信速度低下を防止するため、使用する無線インターフェースだけを「する」に設定してください。

③SSID：……………… ［インターフェース］（①）欄で選択した仮想AP（ath0～ath3）の［SSID］を設定します。
大文字/小文字の区別に注意して、任意の半角英数字32文字以内で入力します。
（出荷時の設定：ath0選択時→CELLCROSS-0
ath1選択時→CELLCROSS-1
ath2選択時→CELLCROSS-2
ath3選択時→CELLCROSS-3）
※［SSID］は、無線ネットワークのグループ分けをするために使用します。
［SSID］の異なる無線LAN端末とは接続できません。
※無線アクセスポイントが無線伝送エリア内に複数存在しているような場合、個々の無線ネットワークグループを［SSID（無線ネットワーク名）］で識別できます。
※「ath0」～「ath3」の仮想APで［SSID］が重複している場合は、その仮想APを使用できません。
※［SSID］と［ESSID］は、同じ意味で使用しています。
本製品以外の無線LAN機器では、［ESSID］と表記されている場合があります。

**「仮想AP」画面で設定を変更するときのご注意**

別の仮想APと併せて設定するときは、〈登録〉、または〈登録して再起動〉を操作してから、別の仮想APを選択してください。
〈登録〉または、〈登録して再起動〉の操作をしないで別の仮想APを選択したときは、変更する前の設定内容に戻ります。

## 7. 「仮想AP」画面

### ■ 仮想AP設定

「無線設定」ー「仮想AP」

**仮想AP設定**

① インターフェース: ath0
② 仮想APを使用: ◯しない ◉する
③ SSID: CELLCROSS-0
④ VLAN ID: 0 VLAN IDを付けない場合は0を入力
⑤ ANY接続拒否: ◉しない ◯する
⑥ 接続端末制限: 63
⑦ アカウンティングを使用: ◉しない ◯する

④**VLAN ID:** ………… [インターフェース](①)欄で選択した仮想AP(ath0〜ath3)が所属する無線グループのID番号を設定します。

(出荷時の設定:0)

設定できる範囲は、「0〜4094」です。

※[VLAN ID]を付けないときは、「0」を設定します。

※異なるID番号のネットワークとは通信できません。

⑤**ANY接続拒否:** …… [インターフェース](①)欄で選択した仮想AP(ath0〜ath3)と「ANY」モード(アクセスポイント自動検索接続機能)で通信する無線LAN端末(アイコム社製無線LANカード:SL-11やSL-110を除く)からの検索や接続の拒否についての設定です。 (出荷時の設定:しない)

出荷時の設定では、接続が簡単になるように、無線LAN端末からの検索や接続を許可しています。

この設定を「する」にした場合、「ANY」モードで通信する無線LAN端末が使用するWindows標準のワイヤレスネットワーク接続、弊社製およびアイコム社製無線LAN端末に付属の設定ユーティリティーから検索されません。

⑥ **接続端末制限：**……… [インターフェース]（①）欄で選択した仮想AP（ath0〜ath3）に同時接続可能な無線LAN端末の台数を設定します。（出荷時の設定：63）
設定できる範囲は、「1〜63」です。
接続制限を設定すると、接続が集中するのを防止（本製品の負荷を分散）できますので、接続集中による通信速度低下を防止できます。

⑦ **アカウンティングを使用：**
……………………… [インターフェース]（①）欄で選択した仮想AP（ath0〜ath3）と通信する無線LAN端末のネットワーク利用状況（接続、切断、MACアドレスなど）を収集してアカウンティングサーバーに送信する機能の使用を設定します。
（出荷時の設定：しない）

## 7.「仮想AP」画面

### ■ 暗号化設定

「無線設定」ー**「仮想AP」**

各仮想AP(ath0～ath3)の暗号化設定をします。

暗号化設定

① ネットワーク認証: オープンシステム・共有キー

② 暗号化方式: なし

※選択する設定内容(①、②)に応じて、上記以外の設定(③ ～ ⑦)を表示(☞P111～P115)します。

**① ネットワーク認証:**

……………………… [暗号化方式](②)欄で選択された暗号化方式を使用する無線LAN端末からのアクセスに対する認証方式を選択します。　(出荷時の設定:オープンシステム・共有キー)

※異なる認証方式の相手とは互換性がありませんので、通信をする相手間で同じ設定にしてください。

**※「MAC認証」、「IEEE802.1X」、「WPA」、「WPA2」、「WPA・WPA2」を選択したときは、RADIUSサーバーによる認証設定が必要です。**

**設定には、下記の2とおりがあります。**

◎仮想AP(ath0～ath3)すべてに同じ認証設定を使用する場合

「認証サーバー」画面にある[RADIUS設定]項目(☞P120、P121)で設定します。

◎仮想AP(ath0～ath3)ごとに異なる認証設定を使用する場合

「仮想AP」画面に表示される[RADIUS設定]項目(☞P116、P117)で設定します。

**【不正アクセス防止のアドバイス】**

本製品に設定する暗号鍵(WEPキー)/共有鍵(Pre-Shared Key)は、容易に推測されないものにしてください。

数字とアルファベット(大文字/小文字)を組み合わせた複雑なものにし、さらに定期的に暗号鍵/共有鍵を変更すると有効です。

①ネットワーク認証:(つづき)

……………………………【認証方式について】

◎**オープンシステム・共有キー:**

「WEP RC4」暗号化方式による無線LAN端末からのアクセスに対して、「オープンシステム」と「共有キー」を自動認識しますので、本製品と暗号鍵(キー)が同じであれば通信できます。

◎**オープンシステム:**

「WEP RC4」暗号化方式による無線LAN端末からのアクセスに対して、暗号鍵(キー)の認証をしません。

◎**共有キー:**

「WEP RC4」暗号化方式による無線LAN端末からのアクセスに対して、本製品と無線LAN端末の暗号鍵(キー)が同じかどうかを認証します。



**【ネットワーク認証と暗号化方式の対応について】**

| | オープンシステム<br>オープンシステム・共有キー | 共有キー | MAC認証 | WPA<br>WPA2<br>WPA-PSK<br>WPA2-PSK | IEEE802.1X |
|---|---|---|---|---|---|
| なし | ○ | × | ○ | × | × |
| WEP RC4 | ○ | ○ | ○ | × | ○ |
| TKIP | × | × | × | ○ | × |
| AES | × | × | × | ○ | × |

## 7.「仮想AP」画面

### ■ 暗号化設定

「無線設定」ー**「仮想AP」**



※選択する設定内容(①、②)に応じて、上記以外の設定(③ ～ ⑦)を表示(☞P111～P115)します。

①ネットワーク認証：(つづき)

…………………………【認証方式について】(つづき)

**◎MAC認証：**

「MAC認証」を選択したときは、RADIUSサーバーによる無線LAN端末のMACアドレスで認証できます。

※「オープンシステム」認証に対応したクライアントが必要です。

※[暗号化方式](②)欄で、「なし」(出荷時の設定)、または「WEP RC4」を選択したとき使用できます。

※RADIUSサーバーによる認証設定(☞P116、P120)が必要です。

※RADIUSサーバーで認証するクライアントのMACアドレスを「00-AB-12-CD-34-EF」とした場合、お使いになるRADIUSサーバーに設定するユーザー名とパスワードは、下記の書式(半角英数字(小文字))で登録してください。

**【書式】**

**ユーザー名：**00ab12cd34ef

**パスワード：**00ab12cd34ef

**下記の書式は、ユーザー名とパスワードに使用できません。**

- 00-ab-12-cd-34-ef　区切り記号( - )の使用
- 00:AB:12:CD:34:EF　区切り記号( : )と英字を大文字で使用
- 00AB12CD34EF　英字を大文字で使用

①ネットワーク認証：（つづき）

……………………………【認証方式について】（つづき）

◎IEEE802.1X：

「WEP RC4」暗号化方式を使用して、RADIUSサーバーによるIEEE802.1X認証するときの設定です。

※「認証サーバー」画面（☞P116、P120）と併せて設定してください。

◎WPA（Wi-Fi Protected Access）：

「TKIP」/「AES」暗号化方式を使用して、RADIUSサーバーによるIEEE802.1X認証をするときの設定です。

※［IEEE802.1X］認証より強力で、「TKIP」暗号化方式の使用を標準規格とする認証方式です。

※「認証サーバー」画面（☞P116、P120）と併せて設定してください。

◎WPA2：

ネットワーク認証方式にWPA2を使用します。

※［WPA］認証より強力な「AES」暗号化方式の使用を標準規格とする認証方式で、「PMKIDキャッシュ」により、再接続による認証が不要です。

※「WPA2」認証に対応したクライアントが必要です。

※「認証サーバー」画面（☞P116、P120）と併せて設定してください。

◎WPA･WPA2：

「WPA」認証と「WPA2」認証を自動認識します。

◎WPA-PSK（Pre-Shared Key）：

共有鍵（キー）で認証します。

RADIUSサーバーを利用しない簡易的な「TKIP」/「AES」暗号化の認証方式で、本製品と無線LAN端末の共有鍵（キー）が同じかどうかを認証します。

◎WPA2-PSK：

ネットワーク認証方式にWPA2-PSKを使用します。

※「WPA2-PSK」認証に対応した無線LAN端末が必要です。

◎WPA-PSK･WPA2-PSK：

「WPA-PSK」認証と「WPA2-PSK」認証を自動認識します。

## 7.「仮想AP」画面

### ■ 暗号化設定

「無線設定」ー**「仮想AP」**



※選択する設定内容(①、②)に応じて、上記以外の設定(③ ~ ⑦)を表示(☞P111~P115)します。

②**暗号化方式:** ………… 無線伝送データを暗号化する方式を選択します。

(出荷時の設定:なし)

対応する暗号化方式は、「WEP RC4」、「TKIP」、「AES」です。

異なる暗号化方式の相手とは互換性がありませんので、暗号化方式は、通信をする相手間で同じ設定にしてください。

※「WEP RC4 152(128)」方式での接続は、弊社製およびアイコム社製無線LAN端末に付属の設定ユーティリティーをご使用ください。

**【暗号化方式について】**

◎**なし:**

データを暗号化しないで通信します。

※[ネットワーク認証](①)欄で、「オープンシステム・共有キー」、「オープンシステム」または「MAC認証」を選択したとき使用できます。

※[IEEE802.11n/a/b/g]規格に準拠します。

※暗号化を設定されることをおすすめします。

**【不正アクセス防止のアドバイス】**

本製品に設定する暗号鍵(WEPキー)/共有鍵(Pre-Shared Key)は、容易に推測されないものにしてください。

数字とアルファベット(大文字/小文字)を組み合わせた複雑なものにし、さらに定期的に暗号鍵/共有鍵を変更すると有効です。

②暗号化方式：………… 【暗号化方式について】（つづき）

◎WEP RC4：

無線通信で一般によく使用されるセキュリティーです。

※暗号鍵(キー)の長さは、64(40)/128(104)/152(128)ビットの中から選択できます。

※[ネットワーク認証](①)欄で、「オープンシステム・共有キー」、「オープンシステム」、「共有キー」、「MAC認証」または「IEEE802.1X」を選択したとき使用できます。

※「WEP RC4 152(128)」方式は、Windows標準のワイヤレスネットワーク接続を使用して本製品に接続できません。

※[IEEE802.11a/b/g]規格に準拠します。

◎TKIP(Temporal Key Integrity Protocol)：

暗号鍵(キー)を一定間隔で自動更新しますので、「WEP RC4」より強力です。

Windows標準のワイヤレスネットワーク接続を使用して本製品に接続できます。

※[ネットワーク認証](①)欄で、「WPA」や「WPA2」、または「WPA-PSK」、「WPA2-PSK」を選択したとき使用できます。

※[IEEE802.11a/b/g]規格に準拠します。

※ご使用いただける「TKIP」対応の弊社製およびアイコム社製無線LAN端末については、「暗号化対応表」(☞P188)をご覧ください。

## 7.「仮想AP」画面

### ■ 暗号化設定

「無線設定」—「仮想AP」

**暗号化設定**

① ネットワーク認証: オープンシステム・共有キー
② 暗号化方式: なし

※選択する設定内容(①、②)に応じて、上記以外の設定(③ ～ ⑦)を表示(☞P111～P115)します。

② 暗号化方式: ………… 【暗号化方式について】(つづき)

◎AES(Advanced Encryption Standard):
暗号化の強化、および暗号鍵(キー)を一定間隔で自動更新しますので、「TKIP」より強力な暗号化方式です。
※[ネットワーク認証](①)欄で、「WPA」や「WPA2」、または「WPA-PSK」、「WPA2-PSK」を選択したとき使用できます。
※[IEEE802.11n/a/b/g]規格に準拠します。
※ご使用いただける「AES」対応の弊社製およびアイコム社製無線LAN端末については、「暗号化対応表」(☞P188)をご覧ください。

◎TKIP・AES:
無線LAN端末からのアクセスに対して、「TKIP」と「AES」を自動認識します。
※[ネットワーク認証](①)欄で、「WPA」や「WPA2」、または「WPA-PSK」、「WPA2-PSK」を選択したとき使用できます。
※「AES」が認識されたときだけ、[IEEE802.11n]規格で通信できます。

## ■ 暗号化設定

「無線設定」ー「**仮想AP**」

**暗号化設定**

| | |
|---|---|
| ① ネットワーク認証: | オープンシステム・共有キー |
| ② 暗号化方式: | WEP RC4 152(128) |
| ③ キージェネレーター: | |
| ④ WEPキー: | 00000000000000000000000000000000<br>半角英数で16文字、もしくは16進数で32桁を入力 |

※選択する設定内容(①、②)に応じて、上記以外の設定(⑤ ～ ⑦)を表示(☞P114～P115)します。

**③キージェネレーター:**

暗号化、および復号に使用する16進数の暗号鍵(キー)を[WEPキー:]欄(④)に生成するための文字列を入力します。　(出荷時の設定:空白《何も設定されていません。》)

※弊社およびアイコム社製以外の機器とは互換性がありませんので、ご注意ください。

**次の順番に操作すると、設定できます。**

**1.** [ネットワーク認証](①)欄で、「オープンシステム･共有キー」、または「オープンシステム」、「共有キー」を選択します。

**2.** [暗号化方式](②)欄で、「WEP RC4 64(40)」、「WEP RC4 128(104)」、「WEP RC4 152(128)」を選択します。

●[キージェネレーター:]欄と[WEPキー:](④)欄を表示します。

**3.** 大文字/小文字の区別に注意して、文字列を[キージェネレーター:]欄に31文字以内(任意の半角英数字/記号)で入力します。

●入力した文字列より生成された16進数の暗号鍵(キー)を[WEPキー](④)欄に表示します。

5

## 7.「仮想AP」画面

### ■ 暗号化設定

「無線設定」ー**「仮想AP」**

暗号化設定
① ネットワーク認証: オープンシステム・共有キー
② 暗号化方式: WEP RC4 152(128)
③ キージェネレーター:
④ WEPキー: 00000000000000000000000000000000
半角英数で16文字、もしくは16進数で32桁を入力

※選択する設定内容(①、②)に応じて、上記以外の設定(⑤ ～ ⑦)を表示(☞P120～P121)します。

③キージェネレーター:(つづき)

………………………… ※暗号鍵(キー)を直接入力する場合は、キージェネレーターに文字列が残っていると、[WEPキー:]欄(④)に直接入力できませんので、削除してください。

※入力する文字列は、通信する相手(弊社製機器)側のキージェネレーターと同じ文字列を設定してください。

※キージェネレーターから生成された暗号鍵(キー)が通信相手間で異なる場合、暗号化されたデータを復号できません。

※[WEPキー](④)欄に表示される暗号鍵(キー)の桁数、および文字数は、[暗号化方式](②)欄の設定によって異なります。(☞P43)

④WEPキー： ………… [キージェネレーター]（③）欄を使用しないで、暗号鍵（キー）を直接設定するとき入力します。

※「0〜9」および「a〜f(またはA〜F)」の16進数、またはASCII文字で、半角入力してください。

※入力する暗号鍵（キー）の桁数は、[暗号化方式]（②）欄を設定したとき表示される桁数（10桁の表示例：0000000000）と同じに設定してください。
ASCII文字で入力する場合は、16進数の半分（例：5文字）で入力してください。

※本製品には、キーインデックスの設定がなく、「1」に相当します。
Windows標準のワイヤレスネットワーク接続を使用して、「WEP RC4」で暗号化された本製品と通信する場合、無線LAN端末側のキーインデックスを「1」に設定してください。
なお、Windows XPでService Packが適用されていない場合は、「0」に設定してください。

## 7.「仮想AP」画面

### ■ 暗号化設定

「無線設定」ー**「仮想AP」**

**暗号化設定**

| | |
|---|---|
| ① ネットワーク認証: | WPA-PSK |
| ② 暗号化方式: | TKIP |
| ⑤ PSK(Pre-Shared Key): | 00000000<br>半角英数で8-63文字、もしくは16進数で64桁を入力 |
| ⑥ WPAキー更新間隔: | 120 分 |

※選択する設定内容(①、②)に応じて、上記以外の設定(③、④、⑦)を表示します。

(☞P111、P113、P115)

**⑤PSK(Pre-Shared Key):**

………………………… 共有鍵(キー)を半角英数字で入力します。

(出荷時の設定:00000000)

※[ネットワーク認証](①)欄で「WPA-PSK」、「WPA2-PSK」、「WPA-PSK･WPA2-PSK」を選択したとき、設定できます。

※同じ暗号化方式を使用する相手と、同じ共有鍵(キー)を設定してください。

※16進数で設定するときは、64桁を入力してください。

※ASCII文字で設定するときは、大文字/小文字の区別に注意して、8文字〜63文字を入力してください。

**⑥WPAキー更新間隔:**

………………………… [ネットワーク認証](①)欄で、「WPA」、「WPA2」、「WPA･WPA2」、「WPA-PSK」、「WPA2-PSK」、「WPA-PSK･WPA2-PSK」を選択したとき、暗号鍵(キー)の更新間隔を分で設定します。 (出荷時の設定:120)
設定できる範囲は、「0〜1440(分)」です。
※「0」を設定すると、更新しません。

## ■ 暗号化設定

「無線設定」ー**「仮想AP」**

**暗号化設定**

| | |
|---|---|
| ① ネットワーク認証: | IEEE802.1X |
| ② 暗号化方式: | WEP RC4 64(40) |
| ⑦ 再認証間隔: | 120 分 |

※選択する設定内容(①、②)に応じて、上記以外の設定(③～⑥)を表示(☞P111～P114)します。

**⑦再認証間隔:** ………… [ネットワーク認証](①)欄で、「MAC認証」または「IEEE802.1X」を選択したとき、RADIUSサーバーに再度認証を要求する間隔を分で設定します。

(出荷時の設定:120)

設定できる範囲は、「0～9999(分)」です。
※「0」を設定したときは、再認証しません。

## 7.「仮想AP」画面

### ■ RADIUS設定

「無線設定」ー**「仮想AP」**

RADIUSサーバーを使用して、MAC認証、WPA認証、WPA2認証、IEEE802.1X認証するときの設定です。

◎[暗号化設定]項目の[ネットワーク認証:]欄(☞P104)で、「MAC認証」、「IEEE802.1X」、「WPA」、「WPA2」、「WPA･WPA2」を選択したとき、表示されます。

◎[仮想AP設定]項目(☞P106)で選択した仮想AP(ath0～ath3)ごとに、異なるRADIUS認証設定ができます。
仮想AP(ath0～ath3)すべてに、同じRADIUS認証設定をする場合は、「認証サーバー」画面の[RADIUS設定]項目(☞P120)で設定してください。

◎EAP-TLSとEAP-TTLS、EAP-PEAPに対応しています。

RADIUS設定

| | | | |
|---|---|---|---|
| ① | 仮想AP毎の設定を使用: | ○しない ◉する | |
| ② | | プライマリー | セカンダリー |
| ③ | アドレス: | | |
| ④ | ポート: | 1812 | 1812 |
| ⑤ | シークレット: | | |

※説明のため、[仮想AP毎の設定を使用:](①)欄を「する」に設定したとき、②～⑤の欄に表示される画面を掲載しています。

**① 仮想AP毎の設定を使用:**

………………………… 仮想AP(ath0～ath3)ごとに、異なる設定でRADIUSサーバーによる認証をするかしないかを設定します。

(出荷時の設定:しない)

※すべての仮想AP(ath0～ath3)に、同じRADIUS認証を設定するときは、「しない」を選択すると、「無線設定」メニューの「認証サーバー」画面で設定する内容が使用できます。

※②～⑤の設定は、「する」を選択するまで表示されません。

② プライマリー/セカンダリー:
………………………… [プライマリー]列に設定したRADIUSサーバーから応答がない場合、その次にアクセスさせるRADIUSサーバーがあるときだけ、[セカンダリー]列に設定(③ ～ ⑤)します。

③ アドレス: …………… 対象となるRADIUSサーバーのIPアドレスを入力します。

④ ポート: ……………… 対象となるRADIUSサーバーの認証ポートを設定します。

(出荷時の設定:1812)

※設定できる範囲は、「1～65535」です。

※ご使用になるシステムによっては、出荷時の設定値と異なることがありますのでご確認ください。

⑤ シークレット: ……… お使いの無線アクセスポイントとRADIUSサーバーの通信に使用するキーを設定します。
RADIUSサーバーに設定された値と同じ設定にします。
半角64文字以内の英数字で入力します。

## 7.「仮想AP」画面

### ■ アカウンティング設定

「無線設定」−**「仮想AP」**

セッション中に使用されたリソースの量(接続、切断、MACアドレスなど)をアカウンティングサーバーに送信する設定です。

◎[仮想AP設定]項目の[アカウンティングを使用:]欄(☞P103)で、「する」を選択したとき、表示されます。

◎[仮想AP設定]項目(☞P100)で選択した仮想AP(ath0〜ath3)ごとに、異なるアカウンティング設定ができます。
仮想AP(ath0〜ath3)すべてに、同じアカウンティング設定をする場合は、「認証サーバー」画面の[アカウンティング設定]項目(☞P122、P123)で設定してください。

アカウンティング設定

| | | |
|---|---|---|
| ①仮想AP毎の設定を使用: | ○しない ◉する | |
| ② | プライマリー | セカンダリー |
| ③アドレス: | | |
| ④ポート: | 1813 | 1813 |
| ⑤シークレット: | | |

※ 説明のため、[仮想AP毎の設定を使用:](①)欄を「する」に設定したとき、② 〜 ⑤の欄に表示される画面を掲載しています。

**① 仮想AP毎の設定を使用:**

............................ 仮想AP(ath0〜ath3)ごとに、異なるアカウンティング設定をするかしないかを設定します。

(出荷時の設定:しない)

※各仮想AP(ath0〜ath3)すべてに、同じアカウンティング設定をするときは、「しない」を選択すると、「認証サーバー」画面の[アカウンティング設定]項目(☞P122、P123)で設定する内容が使用できます。

※② 〜 ⑤の設定は、「する」を選択するまで表示されません。

② **プライマリー/セカンダリー:**
…………………………… [プライマリー]列に設定したサーバーから応答がない場合、その次にアクセスさせるアカウンティングサーバーがあるときだけ、[セカンダリー]列にそのアカウンティングサーバーアドレスを設定(② ~ ④)します。

③ **アドレス:** …………… 対象となるアカウンティングサーバーのIPアドレスを入力します。

④ **ポート:**…………………… 対象となるアカウンティングサーバーのポートを設定します。 (出荷時の設定:1813)
※設定できる範囲は、「1~65535」です。
※ご使用になるシステムによっては、出荷時の設定値と異なることがありますのでご確認ください。

⑤ **シークレット:** ……… この欄に設定されたキーを使用して、本製品とサーバー間の通信をします。
アカウンティングサーバーに設定された値と同じ設定にします。
半角64文字以内の英数字で入力します。

# 8.「認証サーバー」画面

## ■ RADIUS設定

「無線設定」ー**「認証サーバー」**

RADIUSサーバーを使用して、MAC認証、WPA認証、WPA2認証、IEEE802.1X認証するときの設定です。

◎「仮想AP」画面(☞P100)で選択した仮想AP(ath0〜ath3)すべてに、同じRADIUS認証設定ができます。

◎「仮想AP」画面にある[暗号化設定]項目の[ネットワーク認証:]欄(☞P104)で、「MAC認証」、「IEEE802.1X」、「WPA」、「WPA2」、「WPA･WPA2」を選択、[RADIUS設定]項目の[仮想AP毎の設定を使用:]欄(☞P116)で「しない」を選択したとき、設定が有効になります。

◎EAP-TLSとEAP-TTLS、EAP-PEAPに対応しています。

※仮想AP(ath0〜ath3)ごとに、異なるRADIUS認証設定をする場合は、「仮想AP」画面の[RADIUS設定]項目(☞P116)で設定してください。

RADIUS設定

| ① | プライマリー | セカンダリー |
|---|---|---|
| ② アドレス: | | |
| ③ ポート: | 1812 | 1812 |
| ④ シークレット: | | |

① **プライマリー/セカンダリー:**

…………………………… [プライマリー]列に設定したサーバーから応答がない場合、その次にアクセスさせるRADIUSサーバーがあるときは、[セカンダリー]列にそのRADIUSサーバーアドレスを設定します。

② **アドレス:** …………… 対象となるRADIUSサーバーのIPアドレスを入力します。

③ポート:………………… 対象となるRADIUSサーバーの認証ポートを設定します。 (出荷時の設定:1812)

※設定できる範囲は、「1～65535」です。

※ご使用になるシステムによっては、出荷時の設定値と異なることがありますのでご確認ください。

④シークレット: ……… 本製品とRADIUSサーバーの通信に使用するキーを設定します。

RADIUSサーバーに設定された値と同じ設定にします。

半角64文字以内の英数字で入力します。

## 8.「認証サーバー」画面

### ■ アカウンティング設定

「無線設定」−**「認証サーバー」**

セッション中に使用されたリソースの量(接続、切断、MACアドレスなど)をアカウンティングサーバーに送信する設定です。

◎「仮想AP」画面(☞P100)で選択した仮想AP(ath0〜ath3)すべてに、同じアカウンティング設定ができます。

◎「仮想AP」画面にある[仮想AP設定]項目の[アカウンティングを使用:]欄(☞P103)で「する」を選択、[アカウンティング設定]項目の[仮想AP毎の設定を使用:]欄(☞P118)で「しない」を選択したとき、設定が有効になります。

※仮想AP(ath0〜ath3)ごとに、異なるアカウンティング設定をする場合は、「仮想AP」画面の[アカウンティング設定]項目(☞P118、P119)で設定してください。

**アカウンティング設定**

| ① | プライマリー | セカンダリー |
|---|---|---|
| ② アドレス: | | |
| ③ ポート: | 1813 | 1813 |
| ④ シークレット: | | |

**① プライマリー/セカンダリー:**
…………………………… [プライマリー]列に設定したサーバーから応答がない場合、その次にアクセスさせるアカウンティングサーバーがあるときは、[セカンダリー]列にそのアカウンティングサーバーアドレスを設定します。

**② アドレス:** …………… 対象となるアカウンティングサーバーのIPアドレスを入力します。

③ポート:………………… 対象となるアカウンティングサーバーのポートを設定します。（出荷時の設定:1813）
※設定できる範囲は、「1～65535」です。
※ご使用になるシステムによっては、出荷時の設定値と異なることがありますのでご確認ください。

④シークレット: ……… この欄に設定されたキーを使用して、本製品とサーバー間の通信をします。
アカウンティングサーバーに設定された値と同じ設定にします。
半角64文字以内の英数字で入力します。

# 9.「MACアドレスフィルタリング」画面

## ■ MACアドレスフィルタリング設定

「無線設定」ー「MACアドレスフィルタリング」

各仮想AP(ath0〜ath3)に接続できる無線LAN端末を制限する設定です。

MACアドレスフィルタリング設定
① インターフェース: ath0
② MACアドレスフィルタリングを使用: ◉しない ○する
③ フィルタリングポリシー: ◉許可リスト ○拒否リスト

**①インターフェース:**

…………………………… 設定する仮想AP(アクセスポイント)の名称(ath0〜ath3)を選択します。 (出荷時の設定:ath0)

選択するインターフェースごとに、[MACアドレスフィルタリング設定]項目(②、③)と[現在の登録]項目(☞P127)に登録された内容を変更できます。

※表示される名称(ath0〜ath3)は、変更できません。

※使用するときは、[MACアドレスフィルタリングを使用:](②)欄の設定を「する」に変更してください。

※ご使用のWWWブラウザーでJavaScript®が「無効」に設定されていると、「ath0」〜「ath3」を選択したとき、MACアドレスフィルタリング設定]項目(②、③)と[現在の登録]項目に登録された内容が更新されません。
更新されないときは、ご使用のWWWブラウザーでJavaScript®の設定が「有効」に設定されていることを確認してください。

②MACアドレスフィルタリングを使用:

…………………………… [インターフェース:](①)欄で選択した仮想AP(ath0～ath3)について、MACアドレスフィルタリング機能の使用を設定します。 (出荷時の設定:しない)

※「する」に設定すると、[フィルタリングポリシー:](③)欄の設定、および[現在の登録]項目(☞P127)に登録された内容が有効になります。

※選択した仮想APで使用するときは、「仮想AP」画面から該当する仮想APに対する[仮想APを使用:]欄(☞P101)を「する」に設定された仮想APで有効になります。

③フィルタリングポリシー:

…………………………… [現在の登録]項目(☞P127)に登録された無線LAN端末との無線通信を許可するか拒否するかを設定します。

(出荷時の設定:許可リスト)

◎「許可リスト」:MACアドレスが登録された無線LAN端末だけが、本製品と無線通信できます。

※通信を拒否する対象は、MACアドレスを登録していないすべての無線LAN端末です。

◎「拒否リスト」:MACアドレスが登録された無線LAN端末だけが、本製品と無線通信できません。

※通信を許可する対象は、MACアドレスを登録していないすべての無線LAN端末です。

## 9.「MACアドレスフィルタリング」画面

### ■ 端末MACアドレスリスト

「無線設定」－「MACアドレスフィルタリング」

各仮想AP(ath0～ath3)について、MACアドレスフィルタリング(☞P56、P131)の対象となる無線LAN端末のMACアドレスを登録します。

端末MACアドレスリスト
MACアドレス： [ ] 追加

**MACアドレス：** ………… MACアドレスフィルタリングの対象となる無線LAN端末のMACアドレスを入力します。
入力後は、〈追加〉をクリックすると、[現在の登録]項目(☞P127)に表示します。
※対象となる無線LAN端末のMACアドレスが[現在の登録]項目から登録できないときに使用します。
※最大256台分のMACアドレスを登録できます。
※入力は半角英数字で12桁(16進数)を入力します。
※2つの入力例は、同じMACアドレスになります。
(入力例：00-90-c7-00-00-10、0090c7000010)
※[MACアドレスフィルタリング設定]項目の[インターフェース：]欄(☞P124)で選択した仮想AP(ath0～ath3)について、MACアドレスフィルタリングが有効なとき、[現在の登録]項目に登録された無線LAN端末との通信を[フィルタリングポリシー：]欄(☞P125)の設定にしたがって制御します。

## ■ 現在の登録

「無線設定」－「MACアドレスフィルタリング」

各仮想AP(ath0～ath3)について、MACアドレスフィルタリング(☞P49、P125)の対象となる無線LAN端末の登録と通信状態を表示する画面です。

**◆[フィルタリングポリシー:]を「許可リスト」で使用した場合**

現在の 登録

| ①登録済みの端末 | ② 受信中の端末 | ③通信状況 | ④ |
|---|---|---|---|
| | 00-90-C7-00-00-10 | 通信不許可 | 追加 |
| 00-90-C7-00-00-20 | 00-90-C7-00-00-20 | 通信中 | 削除 |
| 00-90-C7-00-00-30 | | 登録済 | 削除 |

**◆[フィルタリングポリシー:]を「拒否リスト」で使用した場合**

現在の 登録

| ①登録済みの端末 | ②受信中の端末 | ③通信状況 | ④ |
|---|---|---|---|
| | 00-90-C7-00-00-10 | 通信中 | 追加 |
| 00-90-C7-00-00-20 | 00-90-C7-00-00-20 | 通信不許可 | 削除 |
| 00-90-C7-00-00-30 | | 登録済 | 削除 |

①**登録済みの端末**……… 登録されている無線LAN端末のMACアドレスを表示します。

②**受信中の端末**………… 本製品の無線伝送領域内で通信している無線LAN端末のMACアドレスを表示します。

③**通信状況**……………… 本製品との無線通信状況を表示します。

「通信中」　：本製品と無線通信中のとき、〈通信中〉とボタンで表示します。
※〈通信中〉をクリックすると、無線通信状態を別画面(☞P129)で表示します。

「通信不許可」：本製品により無線通信が拒否されているときの表示です。

「登録済」　：MACアドレスが登録済みで、無線通信をしていないときの表示です。

5

## 9. 「MACアドレスフィルタリング」画面

### ■ 現在の登録

「無線設定」—「MACアドレスフィルタリング」

◆[フィルタリングポリシー:]を「許可リスト」で使用した場合

現在の登録

| ①登録済みの端末 | ② 受信中の端末 | ③通信状況 | ④ |
|---|---|---|---|
| | 00-90-C7-00-00-10 | 通信不許可 | 追加 |
| 00-90-C7-00-00-20 | 00-90-C7-00-00-20 | 通信中 | 削除 |
| 00-90-C7-00-00-30 | | 登録済 | 削除 |

◆[フィルタリングポリシー:]を「拒否リスト」で使用した場合

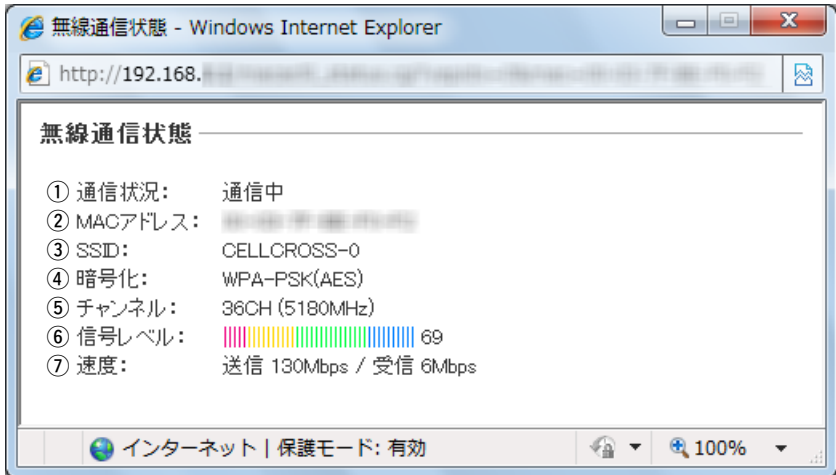
現在の登録

| ①登録済みの端末 | ②受信中の端末 | ③通信状況 | ④ |
|---|---|---|---|
| | 00-90-C7-00-00-10 | 通信中 | 追加 |
| 00-90-C7-00-00-20 | 00-90-C7-00-00-20 | 通信不許可 | 削除 |
| 00-90-C7-00-00-30 | | 登録済 | 削除 |

④**〈追加〉/〈削除〉** ……… [現在の登録]項目に表示されている無線LAN端末のMACアドレスを端末MACアドレスリストに追加、または端末MACアドレスリストから削除するボタンです。

## ■ 無線通信状態

「無線設定」－「MACアドレスフィルタリング」

無線LAN端末との通信状況をモニターします。

※[現在の登録]項目(☞P127)に〈通信中〉ボタンが表示されている場合、そのボタンをクリックすると表示します。

①**通信状況：** ……………「未接続」/「通信中」/「認証中」/「認証失敗」など、接続状況を表示します。
※「通信不可」を表示する場合は、お買い上げの販売店、または販売代理店にお問い合わせください。

②**MACアドレス：**……… 無線LAN端末のMACアドレスを表示します。

③**SSID：** ………………… 無線LAN端末のSSIDを表示します。

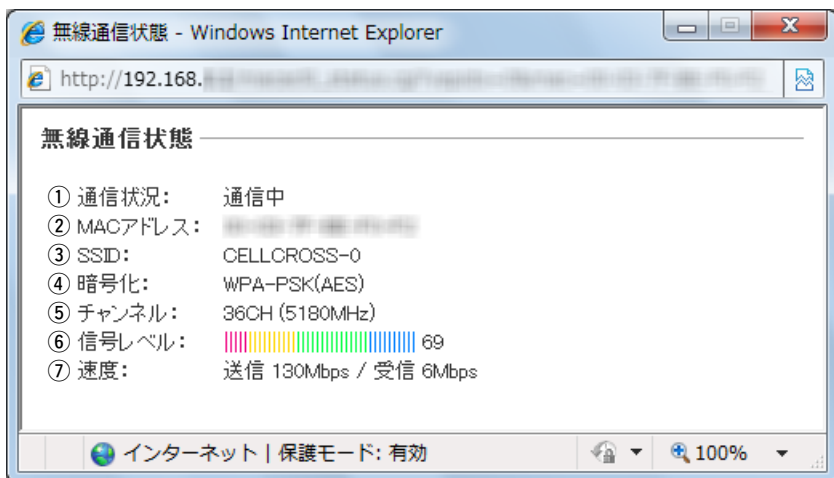
④**暗号化：**………………… 無線LAN端末との通信に使用している認証モード･暗号化方式を表示します。

⑤**チャンネル：** ………… 無線LAN端末との通信に使用しているチャンネルを表示します。

5

## 9. 「MACアドレスフィルタリング」画面

### ■ 無線通信状態

「無線設定」—「MACアドレスフィルタリング」

※[現在の登録]項目(☞P127)に〈通信中〉ボタンが表示されている場合、そのボタンをクリックすると表示します。

**⑥信号レベル：** ………… 無線LAN端末から受信した電波信号の強さを、メーターと数値で表示します。(単位はありません)
安定した通信の目安は、「緑(15)」以上のレベルです。

| 表　示 | [赤] | [黄] | [緑] | [青] |
|---|---|---|---|---|
| レベル | 0～4 | 5～14 | 15～29 | 30以上 |

**【表示される信号レベルの数値について】**
安定した通信の目安は、「緑(15)」以上のレベルです。
ただし、信号レベルが高くても、同じ周波数帯域を使用する無線LAN端末が近くで稼働している場合や無線アクセスポイントの稼働状況などにより、通信が安定しないことがあります。
したがって、あくまでも通信の目安としてご利用ください。

**⑦速度：** …………………… 本製品の通信速度を理論値(Mbps)で表示します。

# 10.「WMM詳細」画面

## ■ WMM詳細設定

「無線設定」ー「WMM詳細」

本製品のWMM機能を使用した無線LAN通信において、[To Station]は、本製品から各無線LAN端末へのデータに対する優先度を設定するEDCA(Enhanced Distributed Channel Access)パラメーターの設定です。

[From Station]は、各無線LAN端末から本製品へのデータに対する優先度を設定するEDCA(Enhanced Distributed Channel Access)パラメーターの設定です。

WMM詳細設定

①通信モード: 802.11ng

To Station

| ②AC Name | ③CWin min | ③CWin max | ④AIFSN(1-15) | ⑥TXOP(0-255) | ⑦No Ack |
|---|---|---|---|---|---|
| AC_BK | 15 | 1023 | 7 | 0 | ☐ |
| AC_BE | 15 | 63 | 3 | 0 | ☐ |
| AC_VI | 7 | 15 | 1 | 94 | ☐ |
| AC_VO | 3 | 7 | 1 | 47 | ☐ |

To Station

| ②AC Name | ③CWin min | ③CWin max | ⑤AIFSN(1-15) | ⑥TXOP(0-255) | ⑧No Ack |
|---|---|---|---|---|---|
| AC_BK | 15 | 1023 | 7 | 0 | |
| AC_BE | 15 | 1023 | 3 | 0 | |
| AC_VI | 7 | 15 | 2 | 94 | ☐ |
| AC_VO | 3 | 7 | 2 | 47 | ☐ |

①**通信モード:** ………… WMM機能の詳細設定(②～⑧)をする無線通信モードを選択します。　(出荷時の設定:802.11ng)

※無線LAN規格(802.11ng/802.11na)ごとに、[To Station]と[From Station]に異なる値を設定できます。

次ページにつづく➔

## 10.「WMM詳細」画面

### ■ WMM詳細設定

「無線設定」ー「WMM詳細」

WMM詳細設定

①通信モード： 802.11ng

To Station

| ②AC Name | ③CWin min | ③CWin max | ④AIFSN(1-15) | ⑥TXOP(0-255) | ⑦No Ack |
|---|---|---|---|---|---|
| AC_BK | 15 | 1023 | 7 | 0 | ☐ |
| AC_BE | 15 | 63 | 3 | 0 | ☐ |
| AC_VI | 7 | 15 | 1 | 94 | ☐ |
| AC_VO | 3 | 7 | 1 | 47 | ☐ |

To Station

| ②AC Name | ③CWin min | ③CWin max | ⑤AIFSN(1-15) | ⑥TXOP(0-255) | ⑧No Ack |
|---|---|---|---|---|---|
| AC_BK | 15 | 1023 | 7 | 0 | |
| AC_BE | 15 | 1023 | 3 | 0 | |
| AC_VI | 7 | 15 | 2 | 94 | ☐ |
| AC_VO | 3 | 7 | 2 | 47 | ☐ |

②**AC Name**： ………… WMM(Wi-Fi Multimedia)で規定されるAC(Access Category)の名称で、各アクセスカテゴリー(AC_BK、AC_BE、AC_VI、AC_VO)ごとに、EDCAパラメーター(③～⑥)を設定できます。
EDCAパラメーター(③～⑥)の各値は、Wi-Fiで定められたアクセスカテゴリーの優先順位[AC_BK(低い)、AC_BE(通常)、AC_VI(優先)、AC_VO(最優先)]となるよう設定されています。

**【ご注意】**
EDCAパラメーター(③～⑥)の各値は、一般的な使用で変更する必要はありません。
なお、変更が必要な場合でも、原則としてWi-Fiで定められたアクセスカテゴリーの優先順位を保つように設定してください。
優先順位を変更した場合、ACM(☞P135)などの制御が正しく動作しない場合があります。

③CWin min/CWin max：

…………………………… CWin(Contention Window)に変更の最小値(min)/最大値(max)を設定します。
チャンネルが一定期間未使用になったあとの送信タイミングをContention Windowから乱数で選択することで、[IEEE802.11]規格でのフレーム衝突を回避します。
設定値が小さいほど優先順位が上がり、設定値が大きいほど優先順位が下がります。

(出荷時の設定：〈To Station〉/〈From Station〉
CWin min→AC_BK(15)
AC_BE(15)
AC_VI(7)
AC_VO(3)
〈To Station〉
CWin max→AC_BK(1023)
AC_BE(63)
AC_VI(15)
AC_VO(7)]
〈From Station〉
CWin max→AC_BK(1023)
AC_BE(1023)
AC_VI(15)
AC_VO(7))

④AIFSN(1-15)：……… Arbitration Interframe Space Number(フレーム送信間隔)を設定します。
設定値が小さいほど、バックオフ制御を開始する時間が早くなるため優先度が高くなります。
設定できる範囲は、「1～15」です。

(出荷時の設定：〈To Station〉
AC_BK(7)
AC_BE(3)
AC_VI(1)
AC_VO(1))

## 10. 「WMM詳細」画面

### ■ WMM詳細設定

「無線設定」ー**「WMM詳細」**

⑤**AIFSN**(2-15)：……… Arbitration Interframe Space Number(フレーム送信間隔)を設定します。
設定値が小さいほど、バックオフ制御を開始する時間が早くなるため優先度が高くなります。
設定できる範囲は、「2～15」です。
（出荷時の設定：〈From Station〉
AC_BK(7)
AC_BE(3)
AC_VI(2)
AC_VO(2)）

⑥TXOP(0-255)：……… チャンネルアクセス権を獲得したあと、排他的にチャンネルの使用を認める期間(Transmission Opportunity)を設定します。
「0」が設定されている場合は、アクセス権獲得後に送信できるフレームは1つになります。
(出荷時の設定：〈To Station〉
AC_BK(0)
AC_BE(0)
AC_VI(94)
AC_VO(47)
〈From Station〉
AC_BK(0)
AC_BE(0)
AC_VI(94)
AC_VO(47))

⑦No Ack：……………… ACK(受信完了通知)による再送信制御についての設定です。
再送信制御をしないときは、チェックボックスにチェックマーク[✔]を入れます。 (出荷時の設定：AC_BK □
AC_BE □
AC_VI □
AC_VO □)

⑧ACM：………………… ACM(Admission Control Mandatory)を設定します。
ACMで保護されたカテゴリーで通信するときは、チェックボックスにチェックマーク[✔]を入れます。
(出荷時の設定：AC_VI □
AC_VO □)
※ACMで保護されたカテゴリーで通信するには、この機能に対応した無線LAN端末の設定が必要です。

## 10. 「WMM詳細」画面

### ■ WMM共通設定

「無線設定」ー「WMM詳細」

IEEE802.11e U-APSD(Unscheduled Automatic Power Save Delivery)機能対応の端末を省電力制御するときの設定です。

WMM共通設定

WMMパワーセーブを使用：　○しない　◉する

**WMMパワーセーブを使用：**

……………………… WMMパワーセーブの使用を設定します。

（出荷時の設定：する）

※「する」に設定すると、無線LAN端末側がWMMパワーセーブ機能を使用したとき、自動的に有効になります。

# 11.「ARP代理応答」画面

## ■ ARP代理応答

「無線設定」ー「ARP代理応答」

無線LAN端末へのARPリクエストに対する応答を代理することで、無線LAN端末の省電力制御をする機能の設定です。

ARP代理応答
① インターフェース： ath0
② ARP代理応答を使用： ◉しない ○する
③ 不明なARPを透過： ○しない ◉する
④ ARPエージング時間： 0 分

**①インターフェース：**

……………………………… 設定する仮想AP(アクセスポイント)の名称を選択します。 (出荷時の設定：ath0)

「ath0」〜「ath3」の仮想APを選択できます。

[ARPキャッシュ情報]項目(☞P139)には、選択した仮想AP(ath0〜ath3)と通信する無線LAN端末の通信を常に監視し、IPv4無線LAN端末のMACアドレスとIPアドレスを表示します。

**②ARP代理応答を使用：**

……………………………… [インターフェース：](①)欄で選択した仮想APについて、ARP代理応答の機能を使用するかしないかを設定します。 (出荷時の設定：しない)

**③不明なARPを透過：**

……………………………… [インターフェース：](①)欄で選択した仮想APと通信している無線LAN端末すべてのARP情報がわかっていて、不明なARPが来たとき、透過するかしないかを設定します。 (出荷時の設定：する)

## 11.「ARP代理応答」画面

### ■ ARP代理応答

「無線設定」－**「ARP代理応答」**



**④ARPエージング時間：**

………………………… 学習したARP情報を削除するまでの時間を設定します。
（出荷時の設定：0）

※ARP情報を学習後、設定した時間が経過すると、該当するARP情報が削除されます。

※「0」（出荷時の設定）のときは、削除されません。

※無線LAN端末が無線アクセスポイント（本製品）から離脱した場合は、時間設定に関わらずARP情報が削除されます。

**【ご参考に】**

**ARPリクエストを受信したとき、アクセスポイントに接続している無線LAN端末のIPアドレス学習状況によって、下記のような処理をします。**

◎ **IPアドレス学習済みの無線LAN端末だけが存在する場合**

ARPリクエストのTargetIPが学習したIPアドレスと一致する場合は、アクセスポイントが代理応答します。

一致しない場合、[不明なARPを透過：]（③）欄の設定が「する」の場合は透過、「しない」の場合は破棄します。

◎**IPアドレスを学習していない無線LAN端末が1台でもいる場合**

ARPリクエストのTargetIPが学習したIPアドレスと一致する場合は、アクセスポイントが代理応答します。

一致しない場合、[不明なARPを透過：]（③）欄の設定に関係なく、ARPリクエストを透過します。

## ■ ARPキャッシュ情報

「無線設定」－「ARP代理応答」

学習したARP情報をMACアドレスとIPアドレスの組み合わせで表示し、必要に応じて削除するための画面です。

①〈削除〉…………………… [ARP代理応答]項目の[インターフェース:]欄(☞P137)で選択したインターフェースが学習したARPキャッシュ情報を削除するボタンです。

②〈一括削除〉…………… [ARP代理応答]項目の[インターフェース:]欄(☞P137)で選択したインターフェースが学習したARPキャッシュ情報を一括して削除するボタンです。

# 12.「WPS」画面

## ■ WPS設定

「無線設定」－「WPS」

WPS(Wi-Fi Protected Setup)機能の使用についての設定です。

※WPS(Wi-Fi Protected Setup)とは、無線LANの[SSID]と[暗号化方式]の設定を容易にするために、「Wi-Fiアライアンス」が提唱する機能です。

WPS設定

① 使用するインターフェース： なし

② 登録 取消 登録して再起動

### ①使用するインターフェース：

WPS機能を使用する仮想AP(ath0～ath3)を設定します。 (出荷時の設定：なし)

※相手の無線LAN端末は、WPS機能対応の製品が必要です。

※ANY接続拒否(☞P102)との併用は、できません。

※使用できる認証方式は、「WPA-PSK･WPA2-PSK」(☞P107)だけです。

※使用できる暗号化方式は、「TKIP･AES」(☞P110)だけです。

※[IEEE802.11n]規格は、「ath0～ath2」の仮想APを設定したときだけです。

※自動設定する[SSID]と[PSK(Pre-Shared Key)]は、本製品側で自動生成(☞P40)、または手動(☞P38、P39)で設定できます。

※2台目の無線LAN端末に自動設定する場合は、すでに本製品に自動設定された内容が配布されます。

②〈登録〉/〈取消〉/〈登録して再起動〉

……………………………… [使用するインターフェース:]欄からインターフェース名(ath0～ath3)を選択後、この画面上で〈登録して再起動〉をクリックします。

※〈登録〉をクリックした状態では、WPS機能の〈開始〉ボタンが[WPS開始]項目(☞P142)に表示されません。

〈取消〉は、「WPS」画面で〈登録〉をクリックする前に変更した内容を元に戻すときクリックします。

## 12.「WPS」画面

### ■ WPS開始

「無線設定」−「WPS」

[SSID]と[暗号化方式]の自動設定を開始するための操作画面です。

**◆[WPS方式:]欄で「プッシュボタン方式」をクリックしたとき**

WPS開始
① WPS方式: ◉プッシュボタン方式 ○PIN方式
② プッシュボタン方式: [開始]

**◆[WPS方式:]欄で「PIN方式」をクリックしたとき**

WPS開始
① WPS方式: ○プッシュボタン方式 ◉PIN方式
③ PIN方式: [　　　] [開始]
相手のPINコードを半角数字8文字で入力

**① WPS方式:** …………… 自動設定の方式を選択します。

（出荷時の方式:プッシュボタン方式）

**「プッシュボタン方式」:**
本製品側で自動生成(☞P40)、または手動(☞P38〜P39)で設定した[SSID]と暗号化の設定を、本製品と無線LAN端末(WPS対応)のワンボタン操作で自動設定する方式です。

**「PIN方式」:**
本製品側で自動生成(☞P40)、または手動(☞P38〜P39)で設定した[SSID]と暗号化の設定を、本製品に設定したPINコード(☞P144)の無線LAN端末(WPS対応)に自動設定する方式です。

※「PIN方式」で無線LAN端末側から本製品を自動設定する場合、本製品のPINコードは、145ページに記載の方法で確認できます。

② **プッシュボタン方式：**

…………………………… プッシュボタン方式で自動設定を開始するための〈開始〉ボタンを表示します。
自動設定を開始するときは、表示された〈開始〉ボタンをクリックします。
※〈開始〉ボタンの表示は、[WPS設定] 項目の[使用するインターフェース：] 欄からインターフェース名(ath0～ath3)を選択後、〈登録して再起動〉をクリックして再起動が完了するまで表示しません。
※自動設定を開始すると、本製品の[MODE] ランプが点滅(緑)します。
自動設定に成功したときは、[MODE] ランプが点灯(緑)します。
※〈開始〉ボタンを操作後、2分以内に、無線LAN端末側の自動設定操作を開始してください。
2分以上経過したり、2台以上の無線アクセスポイントや無線LAN端末が本製品に対してWPSを同時に実行したりしたとき、[MODE] ランプが点滅(赤)して、自動設定を中止しますので、本製品と無線LAN端末の操作をはじめからやりなおしてください。

次ページにつづく➔

## 12. 「WPS」画面

### ■ WPS開始(つづき)

「無線設定」―「WPS」

◆[WPS方式:]欄で「プッシュボタン方式」をクリックしたとき

WPS開始
① WPS方式: ◉プッシュボタン方式 ○PIN方式
② プッシュボタン方式: [開始]

◆[WPS方式:]欄で「PIN方式」をクリックしたとき

WPS開始
① WPS方式: ○プッシュボタン方式 ◉PIN方式
③ PIN方式: [ ] [開始]
相手のPINコードを半角数字8文字で入力

③**PIN方式:**……………… PIN方式で自動設定を開始するための[PINコード入力]欄〈開始〉ボタンを表示します。

※WPSに対応する無線LAN端末のPINコードは、8桁(半角数字)で入力してください。
PINコードが不明な場合は、ご使用になる無線LAN端末に付属する取扱説明書でご確認ください。

※自動設定を開始すると、本製品の[MODE]ランプが点滅(緑)します。
自動設定に成功したときは、[MODE]ランプが点灯(緑)します。

※〈開始〉ボタンを操作後、2分以内に、無線LAN端末側の自動設定操作を開始してください。
2分以上経過したり、2台以上の無線アクセスポイントや無線LAN端末が本製品に対してWPSを同時に実行したりしたとき、[MODE]ランプが点滅(赤)して、自動設定を中止しますので、本製品と無線LAN端末の操作をはじめからやりなおしてください。

## ■ WPS状態表示

「無線設定」–「WPS」

WPS機能で自動設定された内容の確認と削除に使用します。

WPS状態表示

① WPS状態: 設定済 〈初期化して再起動〉

SSID:

ネットワーク認証: WPA-PSK・WPA2-PSK

暗号化方式: TKIP・AES

PSK:

② 〈表示更新〉

① **WPS状態:** …………… WPS機能により自動設定された内容と併せて、その状態を「未設定」/「設定済」/「停止」/「初期化中」で表示します。
※自動設定された内容を削除するときは、〈初期化して再起動〉をクリックします。

② **〈表示更新〉** …………… [WPS状態:](①)欄に表示する内容を更新します。

5

**本製品のPINコードについて**

本製品のPINコード(8桁の半角数字)は、WPS対応の無線LAN端末で生成した[SSID]と[暗号化方式]をPIN方式で本製品に自動設定をするときに必要になります。
必要な場合は、下記のコマンドをtelnet(☞P180)から指定すると確認できます。

▶telnetコマンド:

```
CC-AP1005 # wireless wps enrollee start_pin
Starting WPS PIN method as Enrollee (own_pin=        ).
```

## 13.「管理者」画面

### ■ 管理者パスワードの変更

「システム設定」ー**「管理者」**

本製品の設定画面にアクセスするためのパスワードを変更します。

管理者パスワードの変更

① 管理者ID: admin
② 現在のパスワード:
③ 新しいパスワード:
④ 新しいパスワード再入力:

①**管理者ID:** …………… 本製品の設定画面へのアクセスを許可する管理者IDを表示します。
※本製品の設定画面にアクセスすると、ユーザー名として入力を求められますので、本製品の管理者ID(admin)を入力します。
※本製品の[管理者ID]は、変更できません。

②**現在のパスワード:** …… 新しいパスワードに変更するとき、現在のパスワードを大文字/小文字の区別に注意して入力します。
(出荷時の設定:cellcross)
※入力中の文字は、すべて「*(アスタリスク)」、または「●(黒丸)」で表示します。

**【不正アクセス防止のアドバイス】**

本製品に設定するすべてのパスワードは、容易に推測されないものにしてください。
数字だけでなくアルファベット(大文字/小文字)や記号などを組み合わせた長く複雑なものにし、さらに定期的にパスワードを変更すると有効です。

**【ご注意】**

管理者パスワードを忘れた場合、設定を確認できなくなりますのでご注意ください。
※お忘れの場合、本製品の〈MODE〉ボタンを本書172ページの操作にしたがい、設定を工場出荷時(初期化)の状態に戻していただくことになります。

③新しいパスワード: ……新しいパスワードを入力します。
大文字/小文字の区別に注意して、任意の英数字(半角31文字以内)で入力します。
※新しいパスワードを登録後は、設定内容がマスクされ、すぐにパスワードの入力を求める画面を表示しますので、そこに新しいパスワードを入力します。

④新しいパスワード再入力:
………………………… 確認のために、新しいパスワードを再入力します。

# 14.「管理ツール」画面

## ■ 無線アクセスポイント管理ツール設定

「システム設定」ー**「管理ツール」**

お使いの無線アクセスポイントをRS-AP2(別売品)で集中管理できるようにするための設定です。

| 無線アクセスポイント管理ツール設定 | |
|---|---|
| ① RS-AP2を使用: | ◎しない ◉する |
| ② RS-AP2サーバーアドレス: | |

※説明のため、[RS-AP2:](①)欄で「する」を選択したとき、②の欄に表示される画面を掲載しています。

①**RS-AP2を使用:** …… RS-AP2(アクセスポイント集中管理ツール)から本製品を集中管理できるようにするとき設定します。

(出荷時の設定:しない)

※本製品が集中管理されているあいだは、本製品の設定画面から設定を変更できません。

◎しない　:RS-AP2を使用しなとき

※「しない」に設定されている場合は、RS-AP2から本製品を集中管理できません。

◎する　:RS-AP2を使用するとき

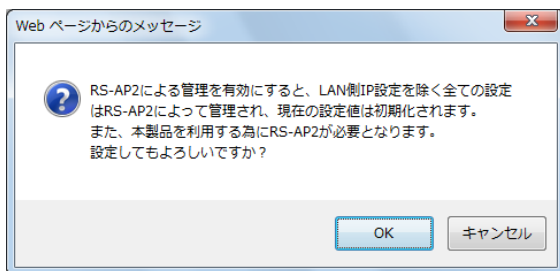
※[RS-AP2サーバーアドレス:](②)欄と併せて設定してください。

※本製品のファームウェアバージョンに関係なく使用できます。

①RS-AP2を使用：(つづき)

**【RS-AP2選択時のご注意】**

「RS-AP2」を選択時、〈登録〉または〈登録して再起動〉をクリックすると、下記の画面を表示します。

**※〈登録して再起動〉をクリックして、下記の画面で〈OK〉をクリックすると、本製品の設定がすべて初期化され、「RS-AP2モード」で動作しますのでご注意ください。**

**※「RS-AP2モード」を解除する場合、初期化操作が必要です。**

次の順番に操作すると、初期化できます。

1. 本製品の電源を切り、本製品からすべてのネットワーク機器を取りはずします。
2. 〈MODE〉ボタンを押しながら、本製品の電源を入れます。
3. [POWER]ランプが点滅(橙色)から点灯(緑色)に切り替わるまで、〈MODE〉ボタンを押しつづけると、初期化完了です。

**②RS-AP2サーバーアドレス：**

RS-AP2を使用するパソコンのIPアドレスを設定します。

※[管理ツールを使用]：(①)欄で「RS-AP2」を選択したとき表示されます。

5

## 14.「管理ツール」画面

### ■ HTTP/HTTPS設定

「システム設定」ー**「管理ツール」**

WWWブラウザーから設定画面にアクセスするためのプロトコルについて設定します。

※ [HTTPを使用:](①)欄と[HTTPSを使用:](②)欄の両方を「しない」に設定すると、WWWブラウザーを使用して、お使いの無線アクセスポイントの設定画面にアクセスできなくなりますのでご注意ください。

HTTP/HTTPS設定

① HTTPを使用：　○しない　◉する

② HTTPSを使用：　◉しない　○する

①**HTTPを使用：** ……… お使いの無線アクセスポイントへのHTTPプロトコルによるアクセスの許可を設定します。

(出荷時の設定:する)

②**HTTPSを使用：** …… 本製品へのHTTPSプロトコルによるアクセスの許可を設定します。　(出荷時の設定:しない)

※HTTPSを使用すると、パスワードやデータが暗号化されるため、TELNETやHTTPでのアクセスより安全性が向上します。

**【HTTP/HTTPS設定設定時のご注意】**

[HTTPを使用:](①)欄と[HTTPSを使用:](②)欄を「しない」に選択時、〈登録〉、または〈登録して再起動〉をクリックしたときは、次の画面を表示します。

※〈登録して再起動〉をクリックして、右記の画面で〈OK〉をクリックすると、「HTTP/HTTPSが共に無効化されました。再起動後はWeb設定画面を利用できません。」が表示され、本製品の設定画面にアクセスできなくなりますのでご注意ください。

※設定画面にアクセスできなくなったときは、本製品にTelnetで接続(☞P180)して、CC-AP1005 #につづけて、下記の太字部分のように入力後、[Enter]キーを押してください。

①CC-AP1005 # **network http on** と入力し[Enter]キーを押します。

②CC-AP1005 # **save** と入力し[Enter]キーを押します。

③CC-AP1005 # **restart** と入力し[Enter]キーを押します。

④本製品の再起動が完了したら、本製品の設定画面へのアクセスを確認します。

## ■ Telnet/SSH設定

「システム設定」ー**「管理ツール」**

TelnetクライアントやSSHクライアントからアクセスするためのプロトコルについて設定します。

Telnet/SSH設定

①Telnetを使用: ○しない ◉する
②SSHを使用: ◉しない ○する
③SSHバージョン: 自動
④SSH認証方式: 自動

① **Telnetを使用:** ……… お使いの無線アクセスポイントへのTelnetプロトコルによるアクセスの許可を設定します。

（出荷時の設定:する）

② **SSHを使用:** ………… お使いの無線アクセスポイントへのSSHプロトコルによるアクセスの許可を設定します。

（出荷時の設定:しない）

※「する」を選択して、[SSH認証方式:]（④）欄で、「自動」/「公開鍵認証」を選択すると、[SSH公開鍵管理]項目(☞P153)と[現在の登録]項目(☞P153)を表示します。

※SSHを使用すると、Telnetクライアントプログラムを使用して設定する内容を暗号化して通信できます。

※SSHを使用するには、別途SSHクライアントをご用意ください。

③ **SSHバージョン:** …… [SSHを使用:]（②）欄で「する」を設定したとき、お使いの無線アクセスポイントで使用するSSH機能のバージョンを設定します。（出荷時の設定:自動）

◎1　:バージョン1を使用します。

◎2　:バージョン2を使用します。

◎自動　:「バージョン1」と「バージョン2」を自動認識します。

## 14. 「管理ツール」画面

### ■ Telnet/SSH 設定

「システム設定」－**「管理ツール」**

Telnet/SSH設定

①Telnetを使用： ○しない ●する

②SSHを使用： ●しない ○する

③SSHバージョン： 自動

④SSH認証方式： 自動

**④ SSH認証方式：**……… [SSHを使用：]（②）欄で「する」を設定したとき、お使いの無線アクセスポイントへのアクセスに対する認証方式を設定します。（出荷時の設定：自動）

◎パスワード認証 ：パスワードを使用して認証するときに設定します。

◎公開鍵認証 ：公開鍵を使用して認証するときに設定します。

◎自動 ：「パスワード認証」と「公開鍵認証」を自動認識します。

## ■ SSH公開鍵管理

「システム設定」ー**「管理ツール」**

SSHでアクセスするときに使用する公開鍵を登録します。
※[Telnet/SSH設定]項目の[SSHを使用:]欄を「する」、[SSH認証方式:]欄を「自動」/「公開鍵認証」に設定したとき表示される項目です。

SSH公開鍵管理

公開鍵ファイル:　[　　　] 参照... 登録
既存の公開鍵は上書きされます

**公開鍵ファイル:**　登録できる鍵は、1種類だけです。

**〈登録の手順〉**

1. 〈参照...〉をクリックして、公開鍵ファイルの保存先を指定します。
2. 〈登録〉をクリックします。
   - ●[現在の登録]項目に公開鍵の内容を表示します。

## ■ 現在の登録

「システム設定」ー**「管理ツール」**

公開鍵ファイルが登録されているとき、公開鍵の内容を表示します。
※[Telnet/SSH設定]項目の[SSHを使用:]欄を「する」、[SSH認証方式:]欄を「自動」/「公開鍵認証」に設定したとき表示される項目です。
※公開鍵ファイルの登録は、[SSH公開鍵管理]項目から登録できます。

※上記画面の内容は、登録例です。

**〈削除〉**……………………　公開鍵ファイルの登録を取り消すボタンです。

# 15.「時計」画面

## ■ 自動時計設定

「システム設定」ー**「時計」**

本製品の内部時計を自動設定するとき、アクセスするタイムサーバーの設定です。

| 自動時計設定 | |
|---|---|
| ①自動時計設定を使用: | ◉しない ○する |
| ②NTPサーバー IPアドレス1: | 210.173.160.27 |
| ③NTPサーバー IPアドレス2: | 210.173.160.57 |
| ④アクセス時間間隔: | 1 日 |
| ⑤前回アクセス日時: | ----/--/-- --:-- |
| ⑥次回アクセス日時: | ----/--/-- --:-- |

**① 自動時計設定を使用:**

………………………… 本製品の自動時計設定機能を設定します。
（出荷時の設定:しない）

「する」に設定すると、インターネット上に存在するタイムサーバーに日時の問い合わせをして、内部時計を自動設定します。

**② NTPサーバーIPアドレス1:**

………………………… アクセスするタイムサーバーのIPアドレスを入力します。 （出荷時の設定:210.173.160.27）

返答がないときは、[NTPサーバーIPアドレス2]（③）欄で設定したタイムサーバーにアクセスします。

※初期に参照しているNTPサーバーは、インターネットマルチフィード株式会社(http://www.jst.mfeed.ad.jp/)のものです。

**③ NTPサーバーIPアドレス2:**

………………………… [NTPサーバー IPアドレス1:]の次にアクセスさせるタイムサーバーがあるときは、そのIPアドレスを入力します。 （出荷時の設定:210.173.160.57）

④ **アクセス時間間隔:**
…………………………… タイムサーバーにアクセスする間隔を設定します。
設定できる範囲は、「1～99(日)」です。
(出荷時の設定:1)
※設定した日数でアクセスできなかったときは、次の間隔までアクセスしません。
※NTPサーバーにアクセスするには、経路を設定する必要があります。
経路を設定しないときは、アクセスできません。
「ネットワーク設定」メニュー→「LAN側IP」画面→[IPアドレス設定]項目にある[デフォルトゲートウェイ:]欄(☞P61)を設定してください。

⑤ **前回アクセス日時:**
…………………………… タイムサーバーにアクセスした日時を表示します。

⑥ **次回アクセス日時:**
…………………………… タイムサーバーにアクセスする予定日時を、[前回アクセス日時](⑤)欄と[アクセス時間間隔](④)欄で設定された日数より算出して表示します。

## 15.「時計」画面

### ■ 内部時計設定

「システム設定」ー「時計」

本製品の内部時計を設定します。

内部時計設定

| | |
|---|---|
| ①本体の時刻: | 2008年 01月 01日 01時 09分 |
| ②設定する時刻: | 2011 年 05 月 31 日 16 時 51 分 ③〈時刻設定〉 |

①**本体の時刻**:………… 本製品に設定されている時刻を表示します。

②**設定する時刻**: ……… 本製品の設定画面にアクセスしたときの時刻を表示します。
※WWWブラウザーの〈更新〉をクリックすると、端末の時計設定を取得して表示します。

③**〈時刻設定〉**…………… [設定する時刻](②)欄に表示された時刻を本製品に設定するボタンです。
※時刻を正確に設定するときは、本製品の設定画面にアクセスしなおすか、WWWブラウザーの〈更新〉をクリックしてから、〈時刻設定〉をクリックしてください。

# 16.「SYSLOG」画面

## ■ SYSLOG設定

「システム設定」ー「SYSLOG」

指定したホストにログ情報などを出力するための設定です。

SYSLOG設定
① DEBUGを使用: ◉しない ○する
② INFOを使用: ○しない ◉する
③ NOTICEを使用: ○しない ◉する
④ ホストアドレス: [ ]

①**DEBUGを使用:** …… 各種デバッグ情報をSYSLOGに出力する設定です。
(出荷時の設定:しない)

②**INFOを使用:** ………… INFOタイプのメッセージをSYSLOGに出力する設定です。
(出荷時の設定:する)

③**NOTICEを使用:** …… NOTICEタイプのメッセージをSYSLOGに出力する設定です。
(出荷時の設定:する)

④**ホストアドレス:** …… SYSLOG機能を使用する場合、SYSLOGを受けるホストのアドレスを入力します。
※ホストは、SYSLOGサーバー機能に対応している必要があります。

## 17.「SNMP」画面

### ■ SNMP設定

「システム設定」ー「SNMP」

TCP/IPネットワークにおいて、ネットワーク上の各ホストから本製品の情報を自動的に収集してネットワーク管理するときの設定です。

SNMP設定
①SNMPを使用: ○しない ●する
②コミュニティーID(GET): public
③場所:
④連絡先:

**①SNMPを使用:**……… 本製品のSNMP機能を設定します。(出荷時の設定:する)「する」に設定すると、本製品の設定情報をSNMP管理ツール側で管理できます。

**②コミュニティーID(GET):**
………………………… 本製品の設定情報をSNMP管理ツール側から読み出すことを許可するIDを、半角31文字以内の英数字で入力します。 (出荷時の設定:public)

**③場所:**…………………… MIB-II(RFC1213)に対応するSNMP管理ツール側で表示される場所を、半角127文字以内の英数字で入力します。

**④連絡先:**………………… MIB-II(RFC1213)に対応するSNMP管理ツール側で表示される連絡先を、半角127文字以内の英数字で入力します。

# 18.「ネットワーク情報」画面

## ■ インターフェースリスト

「情報表示」－「ネットワーク情報」

本製品のネットワークインターフェースとそのIPアドレスについて、その詳細を表示します。

インターフェース リスト

| インターフェース | IPアドレス | サブネットマスク |
|---|---|---|
| lo0 | 127.0.0.1 | 255.255.255.255 |
| mirror0 | 192.168.0.1 | 255.255.255.0 |

## ■ 本体MACアドレス

「情報表示」－「ネットワーク情報」

本製品のMACアドレスを表示します。

MACアドレスは、本製品のようなネットワーク機器がそれぞれ独自に持っている機器固有の番号で、12桁(0090C7××××××)で表示されています。
また、本製品の底面パネルに貼られているシリアルシールにも、同じ内容で記載しています。

## 18.「ネットワーク情報」画面

### ■ 無線LANユニット

「情報表示」―**「ネットワーク情報」**

本製品で使用している仮想AP(ath0〜ath3)の一覧を表示します。

無線LANユニット

| インターフェース | SSID | BSSID |
|---|---|---|
| ath0 | CELLCROSS-0 | 00-90-C7-[illegible] |
| ath1 | CELLCROSS-1 | 02-90-C7-[illegible] |
| ath2 | CELLCROSS-2 | 06-90-C7-[illegible] |
| ath3 | CELLCROSS-3 | 0A-90-C7-[illegible] |

※「無線設定」メニュー→「無線LAN」画面→[無線LAN設定]項目にある[無線UNITを使用:]欄(☞P90)で「しない」を設定している場合は、上記の一覧を表示しません。

※「無線設定」メニュー→「仮想AP」画面→[仮想AP設定]項目にある[仮想APを使用:]欄(☞P101)で「しない」を設定している仮想APのインターフェースは、上記の一覧に表示しません。

### ■ DHCPリース情報

「情報表示」―**「ネットワーク情報」**

本製品のDHCPサーバー機能(☞P54、P62)を使用している場合、有線および無線で本製品に接続する端末に割り当てされたIPアドレスの状態と有効期限を表示します。

DHCPリース 情報

| IPアドレス | MACアドレス | 状態 | リース期限 |
|---|---|---|---|
| 192.168.[illegible] | [illegible] | 動的 | 2011[illegible] |
| 192.168.[illegible] | [illegible] | 静的 | |
| 192.168.[illegible] | [illegible] | 静的 | |

※[状態]欄には、「動的」/「静的」/「解放済」を表示します。

※[リース期限]欄は、[状態]欄が「動的」のときだけ表示されます。

※表示件数に制限はありません。

# 19.「SYSLOG」画面

## ■ SYSLOG

「情報表示」ー「SYSLOG」

本製品がホストに出力するログ情報を表示します。

SYSLOG

現在時刻: 00:17 (起動時間: 0 days

①表示するレベル: ☑DEBUG ☑INFO ☑NOTICE ②最新状態に更新 ③消去

| 日付・時間 | レベル | 内容 |
|---|---|---|
| 01/01 00:17:37 | NOTICE | CC-AP1005 Ver. |

※上図のログ情報は表示例です。

①**表示するレベル:**…… ログ情報の各レベルについて、表示/非表示を選択します。
非表示に設定するときは、非表示にするレベルのチェックボックスをクリックして、チェックマーク[✔]をはずします。 (出荷時の設定:☑ DEBUG
☑ INFO
☑ NOTICE)

②**〈最新状態に更新〉**…… 表示内容を最新の状態にするボタンです。

③**〈消去〉** ……………… 表示されたログ情報を削除するボタンです。

## 20.「無線LANユニット」画面

### ■ アクセスポイント情報

「情報表示」－「無線設定情報一覧」－「無線LANユニット」

下記(① ～ ⑤)の無線アクセスポイント情報を表示します。

アクセスポイント 情報

| | | |
|---|---|---|
| ① | 使用中チャンネル: | 36CH (5180MHz) 20MHz帯域幅モード |
| ② | WMM ACM: | 使用しない |
| ③ | WMMパワーセーブ: | 使用する |
| ④ | 現在時刻: | [illegible] |
| ⑤ | 稼働時間: | 0 days 00:02:03 |

**①使用中チャンネル:**
……………………… 本製品の無線通信に使用するチャンネルの設定と帯域幅モード(20MHz/40MHz)の設定(☞P91)を表示します。

**②WMM ACM:**………… 無線通信に使用するチャンネルについて、WMM機能のACM設定(☞P135)を表示します。

**③WMMパワーセーブ:**
…………………………… 無線通信に使用するチャンネルについて、WMMパワーセーブの設定(☞P136)を表示します。

**④現在時刻:** …………… 本製品の時刻設定(☞P156)を表示します。

**⑤稼働時間:** …………… 本製品の稼働時間を表示します。
※電源を切る、または設定の変更や初期化に伴う再起動で、それまでの稼働時間は初期化されます。

## ■ 仮想AP一覧

「情報表示」ー「無線設定情報一覧」ー「無線LANユニット」

各仮想AP(ath0～ath3)の設定状況を仮想APごとに一覧で表示します。
使用していない仮想APの一覧は、インターフェース欄以外が空白になります。

**仮想AP一覧**

| | 項目 | 値 |
|---|---|---|
| ① | インターフェース | ath0 |
| ② | SSID | CELLCROSS-0 |
| ③ | VLAN ID | 0 |
| ④ | ANY接続拒否 | 使用しない |
| ⑤ | 暗号化 | なし |
| ⑥ | MACアドレスフィルタリング | 使用しない |
| ⑦ | ARP代理応答 | 使用しない |

※「ath0」の一覧を例に説明しています。

**①インターフェース**
………………………… 仮想APの名称(ath0～ath3)を表示します。

**②SSID** ………………… 仮想AP(例:ath0)に設定された[SSID](☞P101)を表示します。

**③VLAN ID** …………… 仮想AP(例:ath0)に設定された[VLAN ID](☞P102)を表示します。

**④ANY接続拒否** ……… 仮想AP(例:ath0)に対する[ANY接続拒否](☞P102)の使用状況を表示します。

**⑤暗号化** ……………… 仮想AP(例:ath0)に設定された[ネットワーク認証](☞P104～P107)と[暗号化方式](☞P108～P110)を表示します。
設定されていないときは、「なし」を表示します。

**⑥MACアドレスフィルタリング**
……………………… 仮想AP(例:ath0)に対する[MACアドレスフィルタリング](☞P124～P128)の使用状況を表示します。

**⑦ARP代理応答** ……… 仮想AP(例:ath0)に対する[ARP代理応答](☞P137)の使用状況を表示します。

# 21.「端末情報」画面

## ■ 端末情報

「情報表示」－「無線設定情報一覧」－**「端末情報」**

本製品の仮想AP(ath0～ath3)と通信する無線LAN端末があるとき、その無線LAN端末との通信情報を表示します。

端末情報

①

現在時刻: 00:21 (稼働時間: 0 days 00:04:15) 最新状態に更新

| ②帰属AP | ③MACアドレス | ④IPアドレス | ⑤通信モード | |
|---|---|---|---|---|
| ath0 | | 192.168 | 802.11na | 詳細 ⑥ |

※上図は、無線LAN端末と通信時の表示例です。

①〈最新状態に更新〉…… 表示内容を最新の状態にするボタンです。

②帰属AP ………………… 無線LAN端末との通信に使用する仮想APの名称(例:ath0)を表示します。

③MACアドレス ……… 本製品と通信する無線LAN端末のMACアドレスを表示します。

④IPアドレス ………… 本製品と通信する無線LAN端末のIPアドレスを表示します。

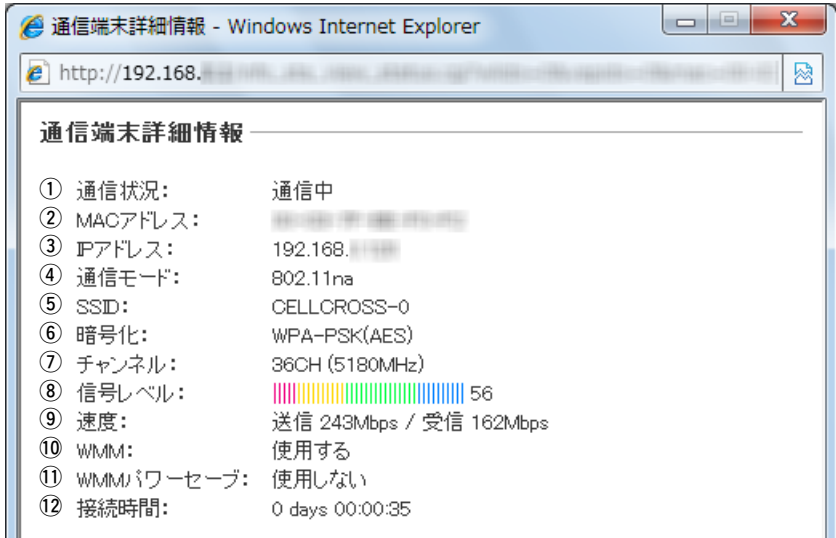
⑤通信モード ………… 無線LAN端末との通信に使用する無線LAN規格を表示します。
◎802.11naを表示する場合
[IEEE802.11n/a(W52)]規格で無線通信しているとき
◎802.11a表示する場合
[IEEE802.11a(W52)]規格で無線通信しているとき
◎802.11ngを表示する場合
[IEEE802.11n/g]規格で無線通信しているとき
◎802.11bgを表示する場合
[IEEE802.11b/g]規格で無線通信しているとき

⑥〈詳細〉………………… 通信中の無線LAN端末の「無線通信詳細情報」を別画面(☞P165)で表示します。

## ■ 通信端末詳細情報

「情報表示」ー「無線設定情報一覧」ー**「端末情報」**

本製品と通信するの無線LAN端末ごとの詳細情報を表示します。

※「MACアドレスフィルタリング」画面の[無線通信状態](☞P135、P136)で表示される内容も含まれています。

※上図は、無線LAN端末と通信中、「端末情報」画面(☞P164)に表示された〈詳細〉ボタンをクリックすると表示します。

①**通信状況:** ……………… 「未接続」/「通信中」/「認証中」/「認証失敗」など、接続状況を表示します。
※「通信不可」を表示する場合は、お買い上げの販売店、または販売代理店にお問い合わせください。

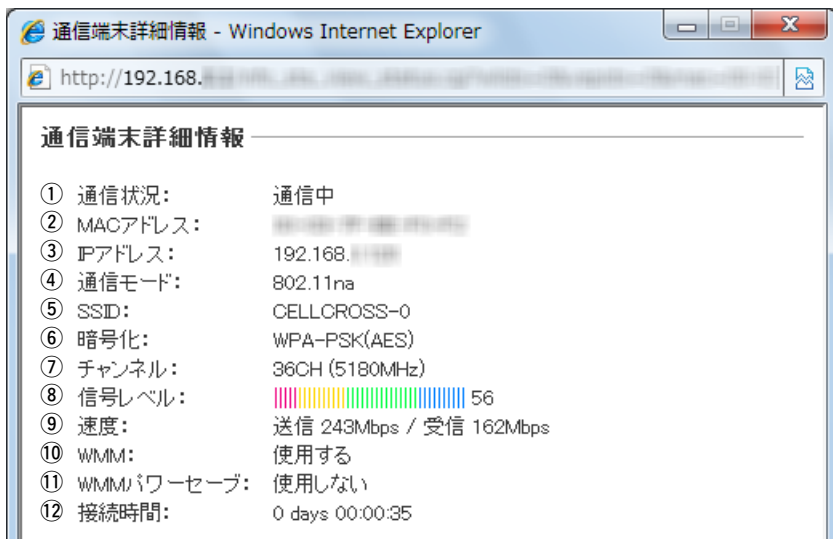
②**MACアドレス:** ……… 無線LAN端末のMACアドレスを表示します。

③**IPアドレス:** ………… 無線LAN端末のIPアドレスを表示します。

5

## 21.「端末情報」画面

### ■ 通信端末詳細情報

「情報表示」ー「無線設定情報一覧」ー**「端末情報」**

※上図は、無線LAN端末と通信中、「端末情報」画面(☞P164)に表示された〈詳細〉ボタンをクリックすると表示します。

④**通信モード:** ………… 無線LAN端末との通信に使用する無線LAN規格を表示します。

◎802.11naを表示する場合
　[IEEE802.11n/a(W52)]規格で無線通信しているとき

◎802.11a表示する場合
　[IEEE802.11a(W52)]規格で無線通信しているとき

◎802.11ngを表示する場合
　[IEEE802.11n/g]規格で無線通信しているとき

◎802.11bgを表示する場合
　[IEEE802.11b/g]規格で無線通信しているとき

⑤SSID: ………………… 無線LAN端末のSSIDを表示します。

⑥暗号化:………………… 無線LAN端末との通信に使用している認証モード･暗号化方式を表示します。

⑦チャンネル: ………… 無線LAN端末との通信に使用しているチャンネルを表示します。

⑧信号レベル: ………… 無線LAN端末から受信した電波信号の強さを、メーターと数値で表示します。(単位はありません)
安定した通信の目安は、「緑(15)」以上のレベルです。

| 表　示 | [赤] | [黄] | [緑] | [青] |
|---|---|---|---|---|
| レベル | 0～4 | 5～14 | 15～29 | 30以上 |

**【表示される信号レベルの数値について】**
安定した通信の目安は、「緑(15)」以上のレベルです。
ただし、信号レベルが高くても、同じ周波数帯域を使用する無線LAN端末が近くで稼動している場合や無線アクセスポイントの稼動状況などにより、通信が安定しないことがあります。
したがって、あくまでも通信の目安としてご利用ください。

⑨速度:…………………… 本製品の通信速度を理論値(Mbps)で表示します。

⑩WMM: ………………… 無線通信に使用するチャンネルについて、WMM機能の使用状況を表示します。

⑪WMMパワーセーブ:
……………………… 無線通信に使用するチャンネルについて、WMMパワーセーブの使用状況を表示します。

⑫接続時間: …………… 無線LAN端末と無線通信した(無通信状態を除く)時間を表示します。
※無線通信しない(無通信)状態がつづいたときは、アクセスしなおしたときからの通信時間が表示されます。

5

# 保守について

# 第 6 章

**この章では、**
**本製品の設定内容保存や初期化、ファームウェアのバージョンアップをする手順について説明しています。**

## 1. 設定内容の確認または保存

本製品の設定画面で変更された内容を確認したり、その内容を設定ファイルとしてパソコンに保存したりできます。

※設定を保存しておくと、誤って設定内容が失われたときなどに利用できます。

### 確認と保存のしかた

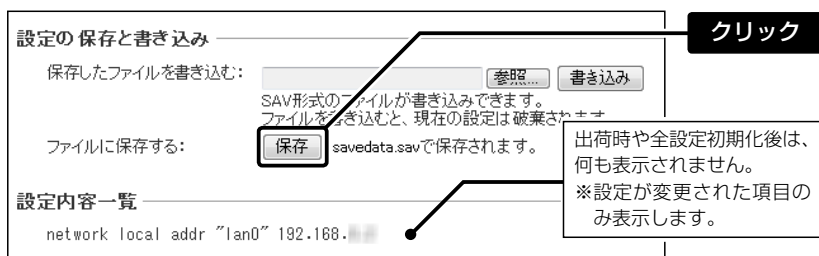
「メンテナンス」→**「設定保存」**

**1** 本製品の設定画面にアクセスします。(☞P36)

**2** 「メンテナンス」メニューをクリックします。

「設定保存」画面を表示します。

**3** [ファイルに保存する]欄の〈保存〉をクリックします。

「ファイルのダウンロード」画面(別画面)を表示します。

**4** 「ファイルのダウンロード」画面の〈保存(S)〉をクリックします。

「名前を付けて保存」画面(別画面)を表示します。

**5** 保存する場所に変更がない場合は、〈保存(S)〉をクリックします。

「.sav」の拡張子がついた設定ファイルが、選択した場所に保存されます。

## 2. 保存された設定の書き込み

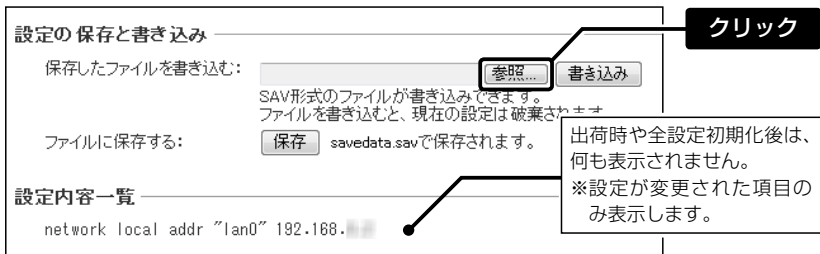
保存した設定ファイル(☞P170)を本製品に書き込む手順を説明します。

### 書き込みかた

「メンテナンス」→「設定保存」

**1** 本製品の設定画面にアクセスします。(☞P36)

**2** 「メンテナンス」メニューをクリックします。
「設定保存」画面を表示します。

**3** 設定ファイルの保存先を指定するため、〈参照...〉をクリックします。
「ファイルの選択」画面(別画面)を表示します。

**4** 「ファイルの選択」画面から保存された設定ファイルを指定して、〈開く(O)〉をクリックします。
[保存したファイルを書き込む:]欄のテキストボックスに、保存先が表示されます。

**5** [設定の保存と書き込み]項目(☞手順3)で、〈書き込み〉をクリックします。
「設定データを復元しています」が表示され、設定ファイルの内容を本製品に書き込みます。

**6** 書き込み後、開いている設定画面を閉じて、設定画面にアクセスしなおします。
現在開いている画面の状態では、書き込まれた設定が反映されません。

**【ご注意】**

本製品の設定ファイルを本製品以外の機種に書き込まないでください。
本製品の設定ファイルを本製品以外の機器に組み込んだり、改変や分解したりしたことによる障害、および本製品の故障、誤動作、不具合、破損、データの消失あるいは停電などの外部要因により通信、通話などの機会を失ったために生じる損害や逸失利益または第三者からのいかなる請求についても当社は一切その責任を負いかねますので、あらかじめご了承ください。

## 3. 設定を出荷時の状態に戻すには

ネットワーク構成を変更するときなど、既存の設定データをすべて消去して、設定をはじめからやりなおすときは、本製品の設定内容を出荷時の状態に戻せます。
そのときの状況に応じて、次の2とおりの方法があります。

A 〈MODE〉ボタンを使用する
※本製品に設定されたIPアドレスが不明な場合など、設定画面にアクセスできないとき

B 設定画面を使用する(☞P173)

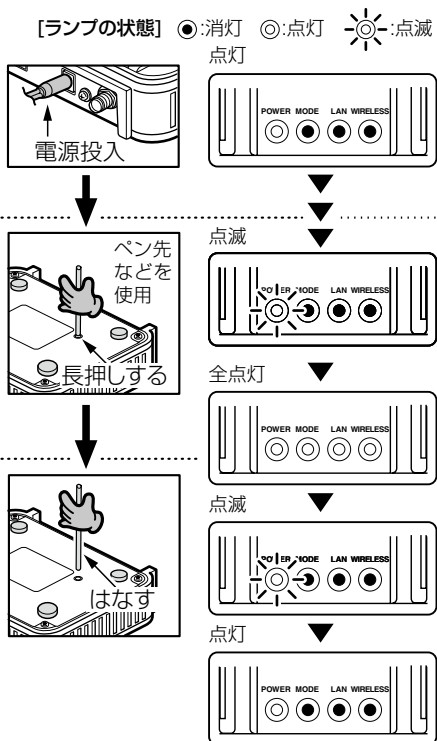
### A 〈MODE〉ボタンを使用する

初期化すると、すべての設定項目が出荷時の状態になります。

パソコンに設定されたIPアドレスのネットワーク部が本製品(出荷時の設定:192.168.0.1)と異なると、設定画面にアクセスできなくなりますので、必要に応じてパソコンのIPアドレスを変更してください。

**1** 本製品からすべてのネットワーク機器を取りはずして、電源を接続します。
※[POWER]ランプの点灯を確認してから手順2の操作を開始してください。

**2** すべてのランプが点灯するまで、〈MODE〉ボタンを押します。

すべてのランプが同時点灯に切り替わったとき、〈MODE〉ボタンから手をはなします。
[POWER]ランプが数回点滅します。
※数秒後、点灯に切り替わると、初期化完了です。

本製品に設定されたIPアドレスがわかっていて、そのIPアドレスで設定画面にアクセスできるときは、本製品の設定画面から、すべての設定を出荷時の状態に戻せます。

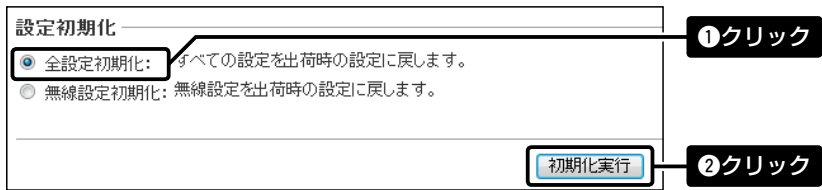
## Ⓑ 設定画面を使用する

「メンテナンス」→「設定初期化」

IPアドレスが不明な場合などの初期化については、本書172ページをご覧ください。

**1** 本製品の設定画面にアクセスします。(☞P36)

**2** 「メンテナンス」メニュー、[設定初期化]の順にクリックします。
「設定初期化」画面を表示します。

**3** 初期化したい条件をクリックして、〈初期化実行〉をクリックします。
クリックした条件に該当する設定内容が出荷時の設定に戻ります。

**4** 再起動完了(約1分)後、[Back]と表示された文字の上にマウスポインターを移動してクリックします。
[ユーザー名]と[パスワード]を求める画面が表示されます。(☞P36)

6

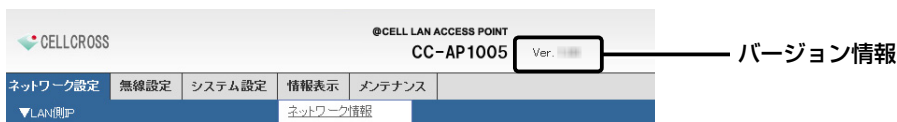
### 初期化の条件について

- **全設定初期化を選択した場合**
  本製品に設定されたすべての内容を出荷時の状態に戻します。
  初期化実行後は、「192.168.0.1(出荷時の設定)」で動作します。
  初期化によって、パソコンに設定されたIPアドレスのネットワーク部が本製品と異なったときは、アクセスできなくなりますので、必要に応じてパソコンのIPアドレスを変更してください。(☞2章)
- **無線設定初期化を選択した場合**
  「無線設定」メニューで設定した内容だけを出荷時の状態に戻します。
  初期化実行後は、「CELLCROSS-0(出荷時の設定)」のSSID、暗号化されない状態で動作します。
  初期化によって、パソコンに設定されたSSIDや暗号化設定が本製品と異なったときは、アクセスできなくなりますので、必要に応じてパソコンの無線LAN設定を変更してください。(☞2章)

## 4. ファームウェアをバージョンアップする

本製品の設定画面からバージョンアップ(更新)できます。

### ファームウェアについて

ファームウェアは、本製品を動作させるために、出荷時から本製品のフラッシュメモリーに書き込まれているプログラムです。
このプログラムは、機能の拡張や改良のため、バージョンアップをすることがあります。
バージョンアップの作業をする前に、本製品の設定画面にアクセスして、次のフレーム内に表示するバージョン情報を確認してください。
バージョンアップをすると、機能の拡張や改良により、本製品を最良の状態にできます。

### バージョンアップについてのご注意

◎ ファームウェアの更新中は、絶対に本体の電源を切らないでください。
途中で電源を切ると、データの消失や故障の原因になります。
できるだけ、有線LAN端末からのバージョンアップをおすすめします。

◎ ご使用のパソコンでファイアウォール機能が動作していると、バージョンアップできないことがあります。
バージョンアップできない場合は、ファイアウォール機能を「無効」にしてください。

◆ 記載する操作の結果については、自己責任の範囲となりますので、次のことを守って作業をはじめてください。
弊社より提供される本製品のアップデート用ファームウェアファイルを、本製品以外の機器に組み込み、改変や分解したことによる障害、および本製品の故障、誤動作、不具合、破損、データの消失あるいは停電などの外部要因により通信、通話などの機会を失ったために生じる損害や逸失利益、または第三者からのいかなる請求についても当社は一切その責任を負いかねますのであらかじめご了承ください。

## ファイルを指定して更新する

「メンテナンス」→「ファームウェアの更新」

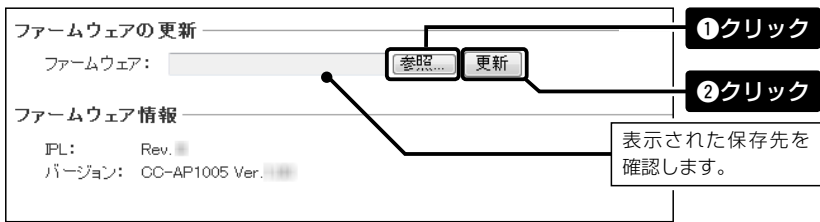
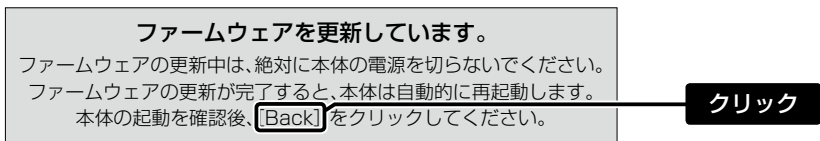
バージョンアップの前に、現在の設定ファイルの保存をおすすめします。(☞P170)

※バージョンアップ後、既存の設定内容が初期化されるファームウェアファイルがありますので、ダウンロードするときは、弊社ホームページに記載の内容をご確認ください。

**1** 本製品の設定画面にアクセスします。(☞P36)

**2** 「メンテナンス」メニュー、[ファームウェアの更新]の順にクリックします。

「ファームウェアの更新」画面を表示します。

**3** 〈参照...〉をクリックして、弊社ホームページよりダウンロードしたファームウェアファイル(拡張子:dat)の保存先を指定してから、〈更新〉をクリックします。

**4** 更新完了(約1分)後、[Back]と表示された文字の上にマウスポインターを移動してクリックすると、設定画面に戻ります。

設定画面に戻らないときは、ファームウェアファイルの更新中ですので、しばらくしてから再度クリックしてください。(接続するパソコンや本製品の電源は、絶対に切らないでください。)

**【ご注意】**

[Back]の操作(☞手順4)で、設定画面に戻るまで、ご使用のパソコンや本製品の電源を絶対に切らないでください。

途中で電源を切ると、データの消失や誤動作の原因になります。

※出荷時の設定内容に戻るような注意書きがあるバージョンアップ用ファームウェアの場合は、[Back]をクリックしても設定画面に戻れませんので、接続するパソコンのIPアドレスを「例:192.168.0.10」に設定してから、本製品の設定画面にアクセスしなおしてください。

6

# ご参考に

# 第７章

**この章では、**
**困ったときの対処法、設定画面の構成、設定項目の初期値、仕様などを説明しています。**

## 1. 困ったときは

下記のような現象は、故障でないことがありますので、修理を依頼される前にもう一度お調べください。

### [POWER]ランプが点灯しない

● **ACアダプターが本製品に接続されていない**
→ ACアダプターおよびDCプラグの接続を確認する

● **ACアダプターをパソコンなどの電源と連動したコンセントに接続している**
→ 本製品のACアダプターを壁などのコンセントに直接接続する

### [LAN]ランプが点灯しない

● **LANケーブルが本製品と正しく接続されていない**
→ 本製品やパソコンの[LAN]ポート、またはLANケーブルを確認する

● **パソコン、またはHUBの電源が入っていない**
→ パソコンとHUBの電源が入っていることを確認する

### 本製品の設定画面にアクセスできない

● **パソコンのIPアドレスを設定していない**
→ 本製品の出荷時や全設定初期化時は、パソコンのIPアドレスを固定IPアドレスに設定する（☞P30～P31）

● **IPアドレスのネットワーク部が、本製品とパソコンで異なっている**
→ パソコンに設定されたIPアドレスのネットワーク部を本製品（☞P37）と同じにする

● **無線LAN設定が、本製品とパソコンで異なっている**
→ パソコンに設定されたネットワーク認証や暗号鍵（キー）を本製品と同じにする

● **ご使用のWWWブラウザーにプロキシサーバーが設定されている**
→ Internet Explorerの「ツール」メニューから「インターネットオプション(O)...」、[接続]タブ、〈LANの設定(L)...〉ボタンの順に操作して、[設定を自動検出する(A)]や[LANにプロキシサーバーを使用する(X)]にチェックマークが入っていないことを確認する

### 本製品の設定画面を正しく表示しない

● **WWWブラウザーのJavaScript機能、およびCookieを無効に設定している**
→ JavaScript機能、およびCookieを有効に設定する（☞P36）

● **Microsoft Internet Explorer7.0以前を使用している**
→ Microsoft Internet Explorer8.0以降を使用する（☞P36）

### [IEEE802.11n]規格で通信できない

● **無線LAN端末が[IEEE802.11n]規格に準拠していない**
→ [IEEE802.11n]規格準拠の無線LAN端末を使用する

● **「AES」以外の暗号化セキュリティーを使用している**
→ 暗号化方式を「AES」に設定する

## [WIRELESS]ランプが点灯しない

● **パソコンの無線LANが機能していない**
→ ご使用のパソコン、または無線LANアダプターに付属の取扱説明書を確認する

● **無線LAN端末と本製品の無線LAN規格が異なっている**
→ [IEEE802.11a(W52)/b/g]規格に準拠した無線LAN端末の使用を確認する

● **[IEEE802.11b/g]規格だけの通信に設定した無線LAN端末を使用している**
→ 本製品の無線チャンネルを[IEEE802.11b/g]規格のチャンネルに変更する(☞P42)

● **本製品の無線LAN機能を無効に設定している**
→ 本製品の無線LAN機能を有効に設定する(☞P90)

● **通信終了後、無線通信しない状態が4分以上つづいた**
→ 本製品に再度アクセスして点灯することを確認する

● **パソコンを起動したあとで、本製品の電源を入れた**
→ 本製品の電源を入れた状態で、パソコンを再起動する

● **無線LAN端末の通信モードが「アドホック」になっている**
→ 無線通信モードを「インフラストラクチャー」に変更する

● **SSID(またはESSID)の設定が異なっている**
→ 本製品と無線LAN端末のSSIDを確認する

● **暗号化認証モードが異なるタイプである**
→ 無線LAN端末、または本製品の認証モードを同じ設定にする

● **MACアドレスフィルタリングを使用している**
→ 無線LAN端末のMACアドレスを本製品に登録する

● **本製品のANY拒否機能を有効に設定している**
→ 本製品のANY拒否機能を無効に設定する

## [WIRELESS]ランプが点灯しているが通信できない

**暗号化セキュリティーの設定が異なっている**
→ 本製品と無線LAN端末の暗号化セキュリティーの設定を確認する

## WPS機能が動作しない(無線LANを自動設定できない)

● **本製品のWPS機能を無効に設定している**
→ WPS機能を使用するインターフェース(ath0〜ath3)を設定していないか、インターフェースの番号を間違えて設定している(☞P140)

● **ほかの無線LAN端末と自動設定中である**
→ ほかの無線LAN端末との自動設定が完了するまで待つ

● **無線LAN端末が無線LANの自動設定に対応していない**
→ WPS対応の弊社製無線LAN端末(例:CC-CA1001)を用意する(☞P187)

● **本製品と無線LAN端末の自動設定操作を2分以内に開始できなかった**
→ 自動設定操作を2分以内に開始する

● **何度繰り返しても、自動設定できない**
→ WPS機能を無効に変更して、手動で設定する(☞P38、P39)

## 2. Telnetで接続するには

Telnetでの接続について説明します。
ご使用のOSやTelnetクライアントが異なるときは、それぞれの使用方法をご確認ください。

### Windows Vista/Windows 7の場合

お使いいただくときは、「コントロールパネル」→「プログラム」→「Windows の機能の有効化または無効化」から、[Telnetクライアント]を有効にしてから、下記の手順で操作してください。

① Windowsを起動します。
② [スタート](ロゴボタン)から[プログラムとファイルの検索]を選択します。
名前欄に「Telnet.exe」と入力し、〈OK〉をクリックします。
※Windows Vistaをご使用の場合は、[スタート](ロゴボタン)から[検索の開始]を選択します。
③ Telnetクライアントが起動しますので、下記のように指定します。
Microsoft Telnet>open 本製品のIPアドレス(入力例:open 192.168.0.1)
④ 下記を入力して、[ENTER]キーを押すと、ログインできます。
**login**:admin
**password**:cellcross
※cellcrossは、本製品の出荷時や全設定初期化時のpasswordです。
※passwordは、本製品の設定画面にある「システム設定」メニューで設定された内容と同じです。
⑤ ログインメッセージ(CC-AP1005 #)が表示されます。

## [CONSOLE]ポートを使用する

本製品の[CONSOLE]ポートとパソコンの[COM]ポートをアイコム社製別売品のケーブル(OPC-1402)で接続すると、ターミナルソフトウェアから設定できます。
使用するときは、パソコンの[COM]ポートを下記の値に設定します。

◎**[接続方法]の選択**：設定用ケーブルを接続している[COM]ポートの番号を指定します。
◎**通信速度**：115200(ビット/秒)
◎**データビット**：8
◎**パリティ**：なし
◎**ストップビット**：1
◎**フロー制御**：なし
※設定後、何も入力せずに[Enter]キーを押すと、「CC-AP1005 #」と表示されます。

## Telnetコマンドについて

本製品で使用できるTelnetコマンドの表示方法と、コマンド入力について説明します。

◎ コマンド一覧 ………………[Tab]キーを押すと、使用できるコマンドの一覧が表示されます。
………………………………コマンド名の入力につづいて[Tab]キーを押すと、サブコマンドの一覧が表示されます。

◎ コマンド名の補完 …………コマンド名を先頭から数文字入力し[Tab]キーを押すと、コマンド名が補完されます。
入力した文字につづくコマンドが1つしかないときは、コマンド名を最後まで補完します。
例) s[Tab]→save
複数のコマンドがあるときは、コマンドの候補を表示します。
例) res[Tab]→reset restart

## 3. 設定項目の初期値一覧

本製品の設定画面について、全設定を初期化したとき表示される各項目の初期値です。

### ネットワーク設定

**「LAN側IP」画面**

**本体名称**
本体名称:CC-AP1005
**VLAN設定**
マネージメントID:0
**IPアドレス設定**
IPアドレス:192.168.0.1
サブネットマスク:255.255.255.0
デフォルトゲートウェイ:空白(設定なし)

**「DHCPサーバー」画面**

**DHCPサーバー設定**
DHCPサーバー機能を使用:しない
割り当て開始IPアドレス:192.168.0.10
割り当て個数:30(個)
サブネットマスク:255.255.255.0
リース期間:72(時間)
ドメイン名:空白(設定なし)
デフォルトゲートウェイ:空白(設定なし)
プライマリーDNSサーバー:空白(設定なし)
セカンダリーDNSサーバー:空白(設定なし)
プライマリーWINSサーバー:空白(設定なし)
セカンダリーWINSサーバー:空白(設定なし)
**静的DHCPサーバー設定**
MACアドレス:空白(設定なし)
IPアドレス:空白(設定なし)

**「ルーティング」画面**

**スタティックルーティング設定**
宛先:空白(設定なし)
サブネットマスク:空白(設定なし)
ゲートウェイ:空白(設定なし)

**「パケットフィルター」画面**

**パケットフィルター**(設定なし)

### 無線設定

**「無線LAN」画面**

**無線LAN設定**
無線UNITを使用:する
チャンネル:036CH (5180MHz)
40MHz帯域幅モード:□(✔なし〈OFF〉)
パワーレベル:-5dB
ストリーム数(Tx×Rx):2×2
最低レート制限:36Mbps
DTIM間隔:1
プロテクション機能:有効

**「仮想AP」画面**(ath0〜ath3)

**仮想AP設定**
インターフェース:ath0
仮想APを使用:する(ath0)
しない(ath1〜ath3)
SSID:CELLCROSS-0(ath0)
CELLCROSS-1(ath1)
CELLCROSS-2(ath2)
CELLCROSS-3(ath3)
VLAN ID:0(ath0〜ath3)
ANY接続拒否:しない(ath0〜ath3)
接続端末制限:63(ath0〜ath3)
アカウンティングを使用:しない(ath0〜ath3)
**暗号化設定**
ネットワーク認証:オープンシステム・共有キー
(ath0〜ath3)
暗号化方式:なし(ath0〜ath3)
※ネットワーク認証の設定に応じて表示される設定項目の初期値については、本書5章をご覧ください。

**「認証サーバー」画面**

**RADIUS設定**(プライマリー／セカンダリー)
アドレス:空白(設定なし)
ポート:1812
シークレット:空白(設定なし)
**アカウンティング設定**
アドレス:空白(設定なし)
ポート:1813(プライマリー／セカンダリー)
シークレット:空白(設定なし)

## 無線設定(つづき)

**「MACアドレスフィルタリング」画面**(ath0〜ath3)
**MACアドレスフィルタリング設定**
インターフェース:ath0
MACアドレスフィルタリングを使用:しない
フィルタリングポリシー:許可リスト
**端末MACアドレスリスト**
MACアドレス:空白(設定なし)

**「WMM詳細」画面**
**WMM詳細設定**
〈To Station〉/〈From Station〉
CWin min:AC_BK(15)、AC_BE(15)
AC_VI(7)、AC_VO(3)
〈To Station〉
CWin max:AC_BK(1023)、AC_BE(63)
AC_VI(15)、AC_VO(7)
〈From Station〉
CWin max:AC_BK(1023)、AC_BE(1023)
AC_VI(15)、AC_VO(7)
〈To Station〉
AIFSN(1-15):AC_BK(7)、AC_BE(3)
AC_VI(1)、AC_VO(1)
〈From Station〉
AIFSN(2-15):AC_BK(7)、AC_BE(3)
AC_VI(2)、AC_VO(2)
〈To Station〉/〈From Station〉
TXOP(0-255):AC_BK(0)、AC_BE(0)
AC_VI(94)、AC_VO(47)
〈To Station〉(✔なし〈OFF〉)
No Ack:AC_BK □、AC_BE □
AC_VI □、AC_VO □
〈From Station〉(✔なし〈OFF〉)
ACM:AC_VI □、AC_VO □
**WMMパワーセーブ設定**
WMMパワーセーブを使用:する

**「ARP代理応答」画面**(ath0〜ath3)
**ARP代理応答**
インターフェース:ath0
ARP代理応答を使用:しない
不明なARPを透過:する
ARPエージング時間:0(分)

**「WPS」画面**
**WPS設定**
使用するインターフェース:ath0
**WPS開始**
WPS方式:プッシュボタン方式

## システム設定

**「管理者」画面**
**管理者パスワードの変更**
管理者ID:admin(変更不可)
現在のパスワード:cellcross(非表示)
新しいパスワード:空白(設定なし)
新しいパスワード再入力:空白(設定なし)

**「管理ツール」画面**
**無線アクセスポイント管理ツール設定**
管理ツールを使用:しない
**HTTP/HTTPS設定**
HTTPを使用:する
HTTPSを使用:しない
**Telnet/SSH設定**
Telnetを使用:する
SSHを使用:しない
SSHバージョン:自動
SSH認証方式:自動

**「時計」画面**
**自動時計設定**
自動時計設定を使用:しない
NTPサーバー IPアドレス1:210.173.160.27
NTPサーバー IPアドレス2:210.173.160.57
アクセス時間間隔:1(日)
※初期に参照しているNTPサーバーは、インターネットマルチフィード株式会社のものです。
http://www.jst.mfeed.ad.jp/
**内部時計設定**
設定する時刻:パソコンから取得した時刻

**「SYSLOG」画面**
**SYSLOG設定**
DEBUGを使用:しない
INFOを使用:する
NOTICEを使用:する
ホストアドレス:空白(設定なし)

**「SNMP」画面**
**SNMP設定**
SNMPを使用:する
コミュニティーID(GET) :public
場所:空白(設定なし)
連絡先:空白(設定なし)

## 4. 設定画面の構成について

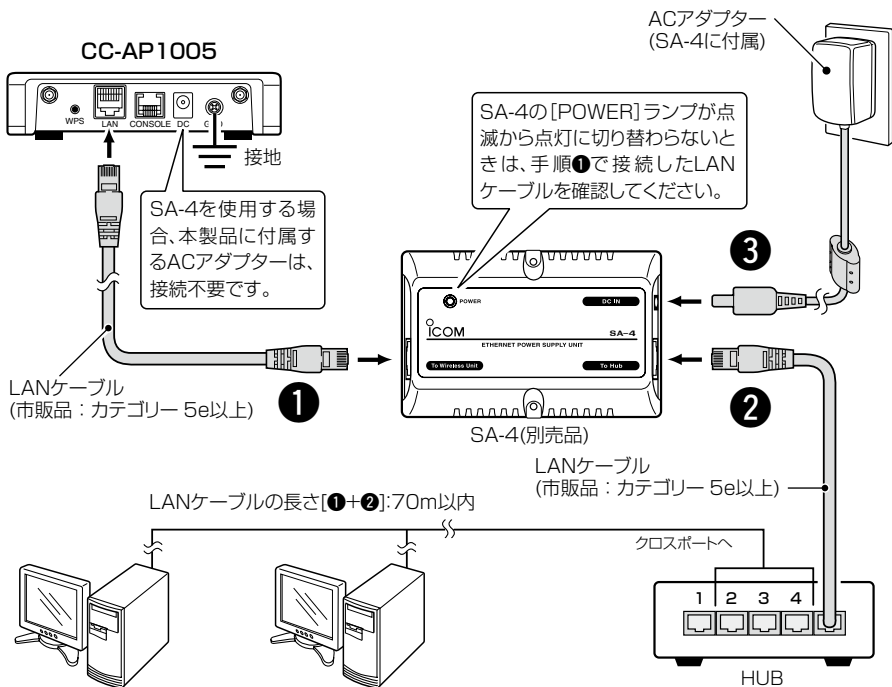
本製品の全設定を初期化したとき、WWWブラウザーに表示される画面構成です。

| 設定メニュー | 設定画面 | 設定項目 |
|---|---|---|
| ネットワーク設定 | LAN側IP | 本体名称 |
| | | VLAN設定 |
| | | IPアドレス設定 |
| | DHCPサーバー | DHCPサーバー設定 |
| | | 静的DHCPサーバー設定 |
| | | 現在の登録 |
| | ルーティング | IP経路情報 |
| | | スタティックルーティング設定 |
| | | 現在の登録 |
| | パケットフィルター | パケットフィルター |
| | | 現在の登録 |
| 無線設定 | 無線LAN | 無線LAN設定 |
| | 仮想AP | 仮想AP設定 |
| | | 暗号化設定 |
| | 認証サーバー | RADIUS設定 |
| | | アカウンティング設定 |
| | MACアドレスフィルタリング | MACアドレスフィルタリング設定 |
| | | 端末MACアドレスリスト |
| | | 現在の登録 |
| | WMM詳細 | WMM詳細設定 |
| | | WMM共通設定 |
| | ARP代理応答 | ARP代理応答 |
| | | ARPキャッシュ情報 |
| | WPS | WPS設定 |
| | | WPS開始 |
| | | WPS状態表示 |
| システム設定 | 管理者 | 管理者パスワードの変更 |
| | 管理ツール | 無線アクセスポイント管理ツール設定 |
| | | HTTP/HTTPS設定 |
| | | Telnet/SSH設定 |
| | 時計 | 自動時計設定 |
| | | 内部時計設定 |
| | SYSLOG | SYSLOG設定 |
| | SNMP | SNMP設定 |

| **設定メニュー**（つづき） | **設定画面** | **設定項目** |
|---|---|---|
| 情報表示 | ネットワーク情報 | インターフェース リスト |
| | | 本体MACアドレス |
| | | 無線LANユニット |
| | | DHCPリース情報 |
| | SYSLOG | SYSLOG |
| 無線設定情報一覧▶ | 無線LANユニット | アクセスポイント情報 |
| | | 仮想AP一覧 |
| | 端末情報 | 端末情報 |
| メンテナンス | 設定保存 | 設定の保存と書き込み |
| | | 設定内容一覧 |
| | 設定初期化 | 設定初期化 |
| | 再起動 | 再起動 |
| | ファームウェアの更新 | ファームウェアの更新 |
| | | ファームウェア情報 |

## 5. PoEによる電源供給について

CC-AP1005の[LAN]ポートに接続されたLANケーブルとSA-4(別売品)を接続して、本製品に電源を供給する接続方法について説明します。

※下記の図に示す番号の順に接続後、SA-4の[POWER]ランプが点滅から点灯状態に切り替わらないときは、手順❶で接続したLANケーブルを確認してください。

### 設置と接続のご注意

◎1台のSA-4で電源供給できるのは、本製品1台だけです。
◎CC-AP1005に付属のACアダプターは必要ありません。
◎SA-4には、電源が必要ですので、コンセントから近い場所に設置してください。
◎HUBなどのネットワーク機器に搭載のリピーター機能は、搭載していません。
したがって、使用するLANケーブルは、HUB(HUBを使用しない場合は、パソコン)からSA-4を介して接続された本製品までの総延長距離が70m以内の場所に設置してください。
※ご使用のLANケーブルによっては、Ethernet規格の最大長制限より短くなることがあります。
◎SA-4は、防水構造ではありませんので、雨水などでぬれやすい場所には設置できません。
◎[1000BASE-T]規格でご使用になる場合、決められた規則にしたがってすべてのピンが結線されたカテゴリー5e以上のLANケーブルをご使用ください。
◎LANケーブルを接続後、SA-4のACアダプターを接続してから、SA-4の[POWER]ランプが点灯に切り替わる(起動する)まで、10秒〜15秒かかることがあります。

## 6. 対応無線LAN製品について

**本製品と無線で通信をするパソコンに装着する無線LAN製品は、弊社およびアイコム社指定の下記のものをご使用ください。 (2011年7月現在)**

◎[IEEE802.11n★1./a(W52)/b/g]規格準拠製品
CC-CA1001(WPS機能対応)、SU-88C(WPS機能対応)、SU-81(WPS機能対応)

◎[IEEE802.11n★1./a(W52/W53/W56)/b/g]規格準拠製品
SE-80(WPS機能対応)、SE-80M(WPS機能対応)、SU-80(WPS機能対応)

◎[IEEE802.11a(W52/W53/W56)/b/g]規格準拠製品
SE-56W

◎[IEEE802.11a(W52/W53)/b/g]規格準拠製品
SL-5200W、SL-5300W、SE-50W、SU-50W

◎[IEEE802.11b/g]規格準拠製品
SL-5000XG★2.、SL-5100★2.、SL-5200★2.、SE-50★2.

◎[IEEE802.11b]規格準拠製品
SL-11、SL-12、SL-110、SL-120、SL-5000、SU-12

※ [IEEE802.11a(J52)]規格の無線LAN端末とは通信できません。
※ アイコム社製無線LANカード(SL-5000XG、SL-5100、SL-5200、SL-5200W、SL-5300W)をご使用になるときは、Card Bus対応のPCカードスロットを装備するパソコンをご用意ください。
※ 今後、弊社およびアイコム社から発売される無線LAN製品については、販売代理店にお問い合わせください。

★1. [IEEE802.11n]規格は、暗号化方式を「なし」または「AES」に設定している場合に有効です。
★2. 法令に基づき、アイコム社での[IEEE802.11a(W52)]規格への移行アップグレードのサービスは、2011年5月31日で終了しました。
[IEEE802.11a(W52)]規格への移行アップグレードを実施されている場合、[IEEE802.11a(W52)/b/g]規格準拠製品としてご使用いただけます。

## 7. 暗号化対応表

弊社製の対応無線LAN製品で使用できる暗号化方式は、下記のとおりです。

| 無線LAN製品 ＼ 暗号化方式 | なし | WEP RC4 | | | TKIP | AES |
|---|---|---|---|---|---|---|
| | | 64bit | 128bit | 152bit | | |
| CC-CA1001 | ○ | ○ | ○ | ○ | ○ | ○ |

アイコム社製の対応無線LAN製品で使用できる暗号化方式は、下記のとおりです。

| 無線LAN製品 ＼ 暗号化方式 | なし | WEP RC4 | | | TKIP | AES |
|---|---|---|---|---|---|---|
| | | 64bit | 128bit | 152bit | | |
| SL-11/SL-110 | ○ | ○ | ○ | × | × | × |
| SL-12/SL-120 | ○ | ○ | ○ | × | × | × |
| SU-12 | ○ | ○ | ○ | × | × | × |
| SL-5000 | ○ | ○ | ○ | ○ | × | × |
| SL-5000XG | ○ | ○ | ○ | ○ | × | × |
| SL-5100 | ○ | ○ | ○ | ○ | × | × |
| SL-5200 | ○ | ○ | ○ | ○ | ○ | ○ |
| SL-5200W | ○ | ○ | ○ | ○ | ○ | ○ |
| SL-5300W | ○ | ○ | ○ | ○ | ○ | ○ |
| SE-50/SE-50W | ○ | ○ | ○ | ○ | ○ | ○ |
| SE-56W | ○ | ○ | ○ | ○ | ○ | ○ |
| SE-80/SE-80W | ○ | ○ | ○ | ○ | ○ | ○ |
| SU-50W | ○ | ○ | ○ | ○ | ○ | ○ |
| SU-80 | ○ | ○ | ○ | ○ | ○ | ○ |
| SU-81 | ○ | ○ | ○ | × | ○ | ○ |
| SU-88C | ○ | ○ | ○ | ○ | ○ | ○ |

※通信相手と暗号化方式や暗号化ビット数が異なるときは、通信できません。
※本製品は、「OCB AES 128bit」に対応していません。
※本製品の[IEEE802.11n] 規格は、「ath0〜ath2」の仮想APを使用し、暗号化方式を「なし」または「AES」に設定している場合に有効です。
※Windows標準のワイヤレスネットワーク接続は、「WEP RC4 152bit」に対応していませんので、弊社製およびアイコム社製無線LAN製品(SU-81を除く)に付属の設定ユーティリティーをご使用ください。また、弊社製およびアイコム社製無線LAN製品(SU-81を除く)に付属の設定ユーティリティーの場合、「TKIP」/「AES」に対応していませんので、Windows標準のワイヤレスネットワーク接続をご使用ください。